AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE 1 OF 3

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
PO49	**04/04/2018 08:33:00 AM**	**21480939**	

6. ISSUED BY	CODE **47QFCA**	7. ADMINISTERED BY (If other than item 6)	CODE
GSA/FEDSIM Acquisition (Q00FB000) **1800 F Street, NW, 3100** **Washington, DC 20405** **Contract Specialist Name: Aaron W Sannutti** **Contract Specialist Phone: 202-705-1719**			

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
GENERAL DYNAMICS ONE SOURCE LLC **3211 JERMANTOWN ROAD** **FAIRFAX, VA, 220302844** **Phone: (703) 246-0624 Fax: (703) 246-0629**		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. **GS00Q09BGD0030 / GST0011AJ0021**
		10B. DATED (SEE ITEM 13) **06/06/2011**
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning ____ copies of the amendment; (b) By acknowledge receipt of this amendment on each of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

285F.Q00FB000.AA10.25.AF151.H08 Total Amount of MOD: $1,000,000.00

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) **FAR 52.232-22, Limitation of Funds**

E. IMPORTANT: Contractor ☒ is not, ☐ is required to sign this document and return ____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of the modification is stated on the attached SF 30 Continuation Page. See attached award documents for details.

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Gregory S Lee	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
		Gregory S Lee	**04/04/2018 08:33:00 AM**
(Signature of person authorized to sign)		(Signature of Contracting Officer)	

		PAGES

Line Item Summary							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	Rev. Ext. Price (F)	Prev. Ext. Price (G)	Amount Of Change (H)
0001A	**Program Management - Base Period 6/6/11-1/27/12 (ARRA)**	(b) (4) (b) (3)					
0001B	**Program Management - Base Period - 1/28/12-6/5/12 (ARRA)**						
0007	**Logistics**						
0008A	**Tools (ARRA)**						
0008B	**Tools (non ARRA)**						
0008C	**Tools (Non ARRA)**						
0008D	**Tools - Option Year 5**						
0008E	**Tools - Option Year 6**						
0009A	**ODCs (ARRA)**						
0009B	**ODCs (non ARRA)**						
0009C	**Tools (Non ARRA)**						
0009D	**ODCs - Option Year 5**						
0009E	**ODCs - Option Year 6**						
0010	**Long Distance Travel**						
0011	**Contract Access Fee**						
1001	**Program Management - Option Period 1 - 6/6/2012 - 6/5/2013**						
1002A	**Phase 1 - Task 2 (Requirements Analysis & Design) (ARRA)**						
1002B	**Phase 1 - Task 2 (Requirements Analysis & Design) (non ARRA)**						
1003A	**Phase 1 - Task 3 (Implement & Test Solution)(ARRA)**						
1003B	**Phase 1 - Task 3 (Implement & Test Solution)(non ARRA)**						
1004A	**Phase 1 - Task 4 (Operations & Maintenance) Year 1**						
1004B	**Phase 1 - Task 4 (Operations and Maintenance) Year 2**						
1007	**Logistics - Option Period 1 - 6/6/2012 - 6/5/2013**						
1011	**Contract Access Fee (CAF) Option Period 1 - 6/6/2012 - 6/5/2013**						
2001	**Program Management - Option Period 2**						
2002A	**Task 2 (Requirements Analysis & Design) (non ARRA)**						
2002B	**Task 2: Requirements Analysis and Design - Option Year 5**						
2002C	**Task 2: Requirements Analysis and Design - Option Year 6**						
2003A	**(Implement & Test Solution)(non ARRA)**						
2003B	**Task 3: Implement and Test Solution - Option Year 5**						
2003C	**Task 3: Implement and Test Solution - Option Year 6**						
2004A	**Task 4: Operations and Maintenance - Option Year 4**						
2004B	**Task 4: Operations and Maintenance - Option Year 5**						

Line Item Summary

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	Rev. Ext. Price (F)	Prev. Ext. Price (G)	Amount Of Change (H)
2004C	Task 4: Operations and Maintenance - Option Year 6	(b) (4)	(b) (3)				
2007	Logistics - Option Period 2						
2011	Contract Access Fee (CAF) Option Period 2						
3001A	Program Management Option Period 3 - 6 Months						
3001B	Program Management Option Period 3 - 6 Months 12/6/14-6/5/15						
3007	Logistics - Option Period 3 - 6/6/14						
3010	Long Distance Travel - Option Year 6: 6 June 2017 to 5 June 2018						
3011	Contract Access Fee (CAF) Option Period 3						
4001A	Program Management Option Period 4						
4001B	Program Management Option Period 4						
4007	Logistics						
4011	Contract Access Fee (CAF) Option Period 4						
5001A	Task 1: Program Management - Option Year 5: 6 June 2016 to 5 December 2016						
5001B	Task 1: Program Management - Option Year 5: 6 December 2016 to 5 June 2017						
5007	Task 7: Logistics - Option Year 5						
5011	Contract Access Fee - Option Year 5						
6001A	Task 1: PMO OY6 POP: 6 JUN 17 - 5 DEC 17						
6001B	Task 1: PMO OY6 POP: 6 DEC 17 to 5 JUN 18						
6007	Task 7: Logistics - Option Year 6						
6011	Contract Access Fee - Option Year 6						
9002A	JCSC Task 2: Non-Severable (Requirements Analysis & Design)						
9002B	CSR Task 2: Non-Severable (Requirements Analysis & Design)						
9002C	Physical Security Non-Severable (Requirements Analysis & Design)						
9003A	JCSC Task 3: Non-Severable (Implement & Test Solution)						
9003B	CSR Task 3: Non-Severable (Implement & Test Solution)						
9003C	Physical Security: Non-Severable (Implement & Test Solution)						
9008A	JCSC Task 8: Non-Severable (Tools)						
9008B	CSR Task 8: Non-Severable (Tools)						
9008C	Physical Security Task 8: Non-Severable (Tools)						
				TOTALS:	$284,314,642.61	$283,314,642.61	$1,000,000.00

The purpose of the modification is to:

1. Incrementally fund CLIN 0008E
2. Update in Section B.9.1 Incremental Funding Limitation of Government's Obligation

1. Update attachment TT, Incremental Funding Chart, by incrementally funding CLIN 0008E as follows:

   - CLIN 0008E funding is increased by (b) (4) (b) (3) from (b) (4) (b) (3) to (b) (4) (b) (3)

2. On page B-16 of the Task Order (TO), Section B.9.1, "Incremental Funding Limitation of Government's Obligation," is updated with the revised estimated funding end date.

As a result of this modification, the Task Order ceiling is unchanged and remains $855,815,756.

Task Order funding is increased by (b) (4) (b) (3) from (b) (4) (b) (3) to (b) (4) (b) (3).

An updated copy of the Task Order is attached and changes are annotated with vertical black lines in the right margin.

The issuing office, FEDSIM Acquisition (QF0BCA), affirms its antecedent Government liability under Task Order No. GST0011AJ0021 and confirms that GDOS shall, upon submission of a final invoice at the time of contract closeout, receive payment in full for any indirect cost increase that results from the variance between GDOS' final incurred cost audit and the provisional rates that were invoiced during the performance of the referenced Task Order.

All other terms and conditions remain unchanged.

TASK ORDER

GST0011AJ0021

Department of Homeland Security (DHS) Technology Integration Program (TIP)

in support of:

issued to:
General Dynamics, One Source
3211 Jermantown Road
Fairfax, VA 22030

Under Alliant Contract: GS00Q09BGD0030

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100
Washington, DC 20405

June 6, 2011

FEDSIM Project Numbers 11024HSM & 11030HSV

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section B of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

B.1 GENERAL DESCRIPTION

The work shall be performed in accordance with all sections of this Task Order and the TIP Contractor's Basic Contract, under which the resulting Task Order will be placed. An acronym listing to support this Task Order is included in Section J, Attachment A.

B.5 CONTRACT ACCESS FEE

GSA operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is (b) (4) (b) (4) of the total price/cost of contractor performance. Each Task Order issued under this contract shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at Task Order award. The following access fee applies to Task Orders issued under this contract. GSA-issued Task Orders in excess of $13.3 million/year are capped at $100,000 per order.

B.6 ORDER TYPE

The TIP Contractor shall perform the effort required by this Task Order on a Firm Fixed Price, Cost Plus Fixed Fee, Cost Plus Award Fee, and Cost Reimbursement basis. No base fee on CPAF is allowable.

B.6.1 CONTRACT TYPE CHANGE

Transition from Cost Plus Award Fee to Fixed Price Incentive Fee (FPIF) to CLINs 1004 and 2004 will be considered post-award. The Government reserves the right to change contract type to FPIF for existing CLINs post-award.

B.7 SERVICES AND PRICES/COSTS

The following abbreviations are used in this price schedule:

NTE: Not To Exceed
CLIN: Contract Line Item Number
ODC: Other Direct Cost
CPAF: Cost Plus Award Fee
CPFF: Cost Plus Fixed Fee
FFP: Firm Fixed Price
FPIF: Fixed Price Incentive Fee

B.7.1 OVERARCHING TASKS:

Mandatory, Firm Fixed Price CLINs:

Program Management:

CLIN	Description	Monthly FFP		Annual FFP
0001	Task 1 – Base year			
0001A	Task 1 – Base Year– 6/6/11 through 01/27/12	(b) (4) (b) (3)		
0001B	Task 1 – Base Year – 01/28/12 through 06/05/12			
	Task 1 – Base Year Total			(b) (4) (b) (3)

Optional, Firm Fixed Price CLINs:

Program Management:

CLIN	Description	Monthly FFP		Annual FFP
1001	Task 1 – Optional Period 1	(b) (4) (b) (3)		
2001	Task 1 – Optional Period 2			
3001A	Task 1 – Optional Period 3: 6 June 2014 to 5 December 2014			
3001B	Task 1 – Optional Period 3: 6 December 2014 to 5 June 2015			
4001A	Task 1 – Optional Period 4: 6 June 2015 to 5 December 2015			
4001B	Task 1 – Optional Period 4: 6 December 2015 to 5 June 2016			
5001	Task 1 – Optional Period 5: 6 June 2016 to 5 June 2017			
5001A	Task 1 – Optional Period 5: 6 June 2016 to 5 December 2016			
5001B	Task 1 – Optional Period 5: 6 December 2016 to 5 June 2017			
6001	Task 1 – Optional Period 6: 6 June 2017 to 5 June 2018			
6001A	Task 1 – Optional Period 6: 6 June 2017 to 5 December 2017			
6001B	Task 1 – Optional Period 6: 6 December 2017 to 5 June 2018			

Optional, Cost Plus Fixed Fee – Term, severable CLINs:

Technical Consulting:

CLIN	**Description**	**Estimated Cost**	**Fixed Fee**	**Total Estimated Cost Plus Fixed Fee**
0005	Task 5 – Base Year	(b) (4) (b) (3)		
1005	Task 5 – Option Year 1			
2005	Task 5 – Option Year 2			
3005	Task 5 – Option Year 3			
4005	Task 5 – Option Year 4: 6 June 2015 to 5 June 2016			
5005	Task 5 – Option Year 5: 6 June 2016 to 5 June 2017			
6005	Task 5 – Option Year 6: 6 June 2017 to 5 June 2018			

Emerging Technology:

CLIN	**Description**	**Estimated Cost**	**Fixed Fee**	**Total Estimated Cost Plus Fixed Fee**
0006	Task 6 – Base Year	(b) (4) (b) (3)		
1006	Task 6 – Option Year 1			
2006	Task 6 – Option Year 2			
3006	Task 6 – Option Year 3			
4006	Task 6 – Option Year 4: 6 June 2015 to 5 June 2016			
5006	Task 6 – Option Year 5: 6 June 2016 to 5 June 2017			
6006	Task 6 – Option Year 6: 6 June 2017 to 5 June 2018			

Logistics:

CLIN	Description	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
0007	Task 7 – Base Year	(b) (4) (b) (3)		
1007	Task 7 – Option Year 1			
2007	Task 7 – Option Year 2			
3007	Task 7 – Option Year 3			
4007	Task 7 – Option Year 4: 6 June 2015 to 5 June 2016			
5007	Task 7 – Option Year 5: 6 June 2016 to 5 June 2017			
6007	Task 7 – Option Year 6: 6 June 2017 to 5 June 2018			

Cost Reimbursable:

CLIN	Description		Total Ceiling Price
0008	**TOOLs Including Indirect Handling Rate** (b) (4)		
0008A	Tools ARRA SubCLIN	NTE	(b) (4) (b) (3)
0008B	Tools Non ARRA SubCLIN	NTE	
0008C	Tools Non ARRA SubCLIN - Option Year 4: 6 June 2015 to 5 June 2016	NTE	
0008D	Tools Non ARRA SubCLIN - Option Year 5: 6 June 2016 to 5 June 2017	NTE	
0008E	Tools Non ARRA SubCLIN - Option Year 6: 6 June 2017 to 5 June 2018	NTE	
0009	**ODCs Including Indirect Handling Rate** (b) (4)		
0009A	ODCs ARRA SubCLIN	NTE	
0009B	ODCs Non ARRA SubCLIN	NTE	
0009C	ODCs Non ARRA SubCLIN - Option Year 4: 6 June 2015 to 5 June 2016	NTE	
0009D	ODCs Non ARRA SubCLIN - Option Year 5: 6 June 2016 to 5 June 2017	NTE	
0009E	ODCs Non ARRA SubCLIN - Option Year 6: 6 June 2017 to 5 June 2018	NTE	
0010	Long Distance Travel	NTE	
1010	Long Distance Travel - Option Year 4: 6 June 2015 to 5 June 2016	NTE	

2010	Long Distance Travel - Option Year 5: 6 June 2016 to 5 June 2017	NTE	(b) (4) (b) (3) [redacted]
3010	Long Distance Travel - Option Year 6: 6 June 2017 to 5 June 2018	NTE	
0011	Contract Access Fee – Base Period	NTE	
1011	Contract Access Fee - Option Period 1	NTE	
2011	Contract Access Fee - Option Period 2	NTE	
3011	Contract Access Fee - Option Period 3	NTE	
4011	Contract Access Fee - Option Year 4: 6 June 2015 to 5 June 2016	NTE	
5011	Contract Access Fee - Option Year 5: 6 June 2016 to 5 June 2017	NTE	
6011	Contract Access Fee - Option Year 6: 6 June 2017 to 5 June 2018	NTE	

B.7.2 PHASES

B.7.2.1 PHASE 1:

Mandatory, Cost Plus Award Fee CLINs:

Requirements Analysis and Design,–

CLIN	Description	Estimated Cost	Estimated Award Fee	Total Estimated Cost Plus Award Fee
1002	Task 2, Phase 1	(b) (4) (b) (3) [redacted]		
1002A	Task 2, Phase 1 ARRA Sub CLIN			
1002B	Task 2, Phase 1 Non ARRA Sub CLIN			

Optional, Cost Plus Award Fee CLINs:

Implement and Test Solution

CLIN	Description	Estimated Cost	Estimated Award Fee	Total Estimated Cost Plus Award Fee
1003	Task 3, Phase 1	(b) (4) (b) (3) [redacted]		
1003A	Task 3 ARRA Sub CLIN			
1003B	Task 3 Non ARRA Sub CLIN			

Operations and Maintenance

CLIN	Description	Estimated Cost	Estimated Award Fee	Total Estimated Cost Plus Award Fee
1004A	Task 4 – Year 1	(b) (4) (b) (3)		
1004B	Task 4 – Year 2			

Task 2 and 3 are non-severable. Task 4 is severable.

TOTAL PHASE 1 CLINS: $145,722,185

B.7.2.2 POST PHASE 1: OPTIONAL, COST PLUS AWARD FEE CLINS:

CLIN 2002 – Task 2, Requirements Analysis and Design

CLIN	Description	Estimated Cost	Estimated Award (b) (4) (b)	Total Estimated Cost Plus Award Fee
2002	Task 2, Post Phase 1	(b) (4) (b) (3)		
2002A	Task 2 – Option Year 4: 6 Jun 2015 to 5 Jun 2016			
2002B	Task 2 – Option Year 5: 6 Jun 2016 to 5 Jun 2017			
2002C	Task 2 – Option Year 6: 6 Jun 2017 to 5 Jun 2018			

CLIN 2003 – Task 3, Implement

CLIN	Description	Estimated Cost	Estimated Award (b) (4) (b)	Total Estimated Cost Plus Award Fee
2003	Task 3 - Post Phase 1	(b) (4) (b) (3)		
2003A	Task 3 - Option Year 4: 6 Jun 2015 to 5 Jun 2016			
2003B	Task 3 - Option Year 5: 6 Jun 2016 to 5 Jun 2017			
2003C	Task 3 - Option Year 6: 6 Jun 2017 to 5 Jun 2018			

CLIN 2004- Task 4, Operations and Maintenance

CLIN	Description	Estimated Cost	Estimated Award (b) (4) (b)	Total Estimated Cost Plus Award Fee
2004	Task 4 - Post Phase 1	(b) (4) (b) (3)		
2004A	Task 4 - Option Year 4: 6 Jun 2015 to 5 Jun 2016			
2004B	Task 4 - Option Year 5: 6 Jun 2016 to 5 Jun 2017			
2004C	Task 4 - Option Year 6: 6 Jun 2017 to 5 Jun 2018			

Tasks 2, 3 and 4 are severable.

B.7.2.3 POST PHASE 1: NON-SEVERABLE, CLINS:

CLIN 9002 - Task 2, Requirements Analysis and Design:
Cost Plus Award Fee (CPAF)

CLIN	Description	Estimated Cost	Estimated Award (b) (4) (b)	Total Ceiling Price
9002A	JCSC Task 2: Non-Severable (Requirements Analysis & Design)	(b) (4) (b) (3)		
9002B	CSR Task 2: Non-Severable (Requirements Analysis & Design)			
9002C	Physical Security Non-Severable (Requirements Analysis & Design)			

CLIN 9003 - Task 3, Implement and Test Solution:
Cost Plus Award Fee (CPAF)

CLIN	Description	Estimated Cost	Estimated Award (b) (4) (b)	Total Ceiling Price
9003A	JCSC Task 3: Non-Severable (Implement & Test Solution)	(b) (4) (b) (3)		
9003B	CSR Task 3: Non-Severable (Implement & Test Solution)			
9003C	Physical Security: Non-Severable (Implement & Test Solution)			

CLIN 9008 - Task 8, Tools:
Cost Reimbursable (CR)

CLIN	Description		Total Ceiling Price
9008A	JCSC Task 8: Non-Severable (Tools) / Indirect Handling Rate 8.08%)	NTE	(b) (4) (b) (3)
9008B	CSR Task 8: Non-Severable (Tools) / Indirect Handling Rate (b) (4)	NTE	
9008C	Physical Security Task 8: Non-Severable (Tools) / Indirect Handling Rate (b) (4)	NTE	

TOTAL Post Phase 1 CLINS: (b) (4) (b) (3)

B.7.3 SUMMARY COST TABLE BY CONTRACT TYPE

Firmed Fixed Price CLIN Total	(b) (4) (b) (3)
Cost Plus Fixed Fee CLIN Total	
Cost Plus Award Fee CLIN Total	
Cost Reimbursable CLIN Total	
Contract Access Fee	
GRAND TOTAL ALL CLINS	**$ 855,815,756**

B.8 SECTION B TABLES

B.8.1 INDIRECT/MATERIAL HANDLING RATE

Tools and ODC costs incurred may be burdened with the TIP Contractor's DCAA Forward Price Rate Agreement.

B.8.2 DIRECT AND INDIRECT RATES

B.8.2.1 DIRECT LABOR RATES

All Alliant Prime Contractor direct labor rates under this task order shall be established as "ceiling rates". Labor categories proposed shall be mapped to existing Alliant labor categories. Ceiling rates represents the maximum direct labor rates to be proposed and/or billed under this task order. These ceiling rates apply to cost reimbursable CLINs. The ceiling rates should anticipate the maximum technical expertise needed over the life of the task order and are not necessarily bound by current staff.

B.8.2.2 INDIRECT LABOR RATES

All indirect rates proposed and billed under this task order shall be commensurate with the then current DCAA approved forward pricing rate agreement. Indirect rates include, but may not be limited to, indirect material handling rates, overhead rates, and general and administrative rates.

B.8.2.3 CEILING RATES - GOVERNMENT SITE

TIP CONTRACTOR TO COMPLETE FOR PROPOSED LABOR CATEGORIES.

Alliant Labor Categories	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Contract Year 6	Contract Year 7
Administration/Clerical	(b) (4) (b) (3)						
Administration/Clerical (Entry Level)							
Administration/Clerical (Journeyman)							
Administration/Clerical (Senior)							
Applications Developer							
Applications Developer (Entry Level)							
Applications Developer (Journeyman)							
Applications Developer (Senior)							
Applications Developer (Master)							
Applications Systems Analyst							
Applications Systems Analyst (Entry Level)							
Applications Systems Analyst (Journeyman)							
Applications Systems Analyst (Senior)							

	(b) (4) (b) (3)
Applications Systems Analyst (Master)	[redacted]
Business Process Consultant	
Business Systems Analyst	
Chief Information Security Officer	
Computer Scientist	
Computer Forensic and Intrusion Analyst	
Configuration Management Specialist	
Configuration Management Specialist (Journeyman)	
Configuration Management Specialist (Senior)	
Configuration Management Specialist (Master)	
Data Architect	
Data Warehousing Specialist	
Data Warehousing Specialist (Entry Level)	
Data Warehousing Specialist (Journeyman)	
Data Warehousing Specialist (Senior)	
Data Warehousing Specialist (Master)	
Database Specialist	
Database Specialist (Entry Level)	
Database Specialist (Journeyman)	
Database Specialist (Senior)	
Database Specialist (Master)	
Disaster Recovery Specialist	
Disaster Recovery Specialist (Journeyman)	
Disaster Recovery Specialist (Senior)	
Enterprise Architect	
ERP Analyst	
ERP Business/Architectural Specialist	
Financial Analyst	
GIS Analyst/Programmer	
Graphics Specialist	
Groupware Specialist	
Hardware Engineer	
Hardware Engineer (Entry Level)	
Hardware Engineer (Journeyman)	
Hardware Engineer (Senior)	
Hardware Engineer (Master)	
Helpdesk Specialist	
Helpdesk Specialist (Entry Level)	
Helpdesk Specialist (Journeyman)	
Helpdesk Specialist (Senior)	

	(b) (4) (b) (3)
Information Assurance/Security Specialist	
Information Assurance/Security Specialist (Entry Level)	
Information Assurance/Security Specialist (Journeyman)	
Information Assurance/Security Specialist (Senior)	
Information Assurance/Security Specialist (Master)	
Information Specialist/Knowledge Engineer	
Modeling and Simulation Specialist	
Network Specialist	
Network Specialist (Entry Level)	
Network Specialist (Journeyman)	
Network Specialist (Senior)	
Network Specialist (Master)	
Program Manager	
Project Manager	
Quality Assurance Specialist	
Quality Assurance Specialist (Entry Level)	
Quality Assurance Specialist (Journeyman)	
Quality Assurance Specialist (Senior)	
Quality Assurance Specialist (Master)	
Research Analyst	
Strategic/Capital Planner	
Subject Matter Expert	
Subject Matter Expert (Journeyman)	
Subject Matter Expert (Senior)	
Subject Matter Expert (Master)	
Systems Engineer	
Technical Editor	
Technical Writer	
Test Engineer	
Test Engineer (Entry Level)	
Test Engineer (Journeyman)	
Test Engineer (Senior)	
Training Specialist	
Training Specialist (Entry Level)	
Training Specialist (Journeyman)	
Training Specialist (Senior)	
Voice/Data Communications Engineer	
Voice/Data Communications Engineer (Entry Level)	
Voice/Data Communications Engineer	

(Journeyman)	(b) (4) (b) (3) [redacted]
Voice/Data Communications Engineer (Senior)	
Voice/Data Communications Engineer (Master)	
Web Content Analyst	
Web Designer	

B.8.2.4 CEILING RATES - CONTRACTOR SITE

TIP Contractor to complete for proposed labor categories.

Alliant Labor Categories	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Contract Year 6	Contract Year 7
Administration/Clerical	(b) (4) (b) (3) [redacted]						
Administration/Clerical (Entry Level)							
Administration/Clerical (Journeyman)							
Administration/Clerical (Senior)							
Applications Developer							
Applications Developer (Entry Level)							
Applications Developer (Journeyman)							
Applications Developer (Senior)							
Applications Developer (Master)							
Applications Systems Analyst							
Applications Systems Analyst (Entry Level)							
Applications Systems Analyst (Journeyman)							
Applications Systems Analyst (Senior)							
Applications Systems Analyst (Master)							
Business Process Consultant							
Business Systems Analyst							
Chief Information Security Officer							
Computer Scientist							
Computer Forensic and Intrusion Analyst							
Configuration Management Specialist							
Configuration Management Specialist (Journeyman)							
Configuration Management Specialist (Senior)							
Configuration Management Specialist (Master)							
Data Architect							
Data Warehousing Specialist							
Data Warehousing Specialist (Entry Level)							
Data Warehousing Specialist (Journeyman)							
Data Warehousing Specialist (Senior)							

	(b) (4) (b) (3)
Data Warehousing Specialist (Master)	
Database Specialist	
Database Specialist (Entry Level)	
Database Specialist (Journeyman)	
Database Specialist (Senior)	
Database Specialist (Master)	
Disaster Recovery Specialist	
Disaster Recovery Specialist (Journeyman)	
Disaster Recovery Specialist (Senior)	
Enterprise Architect	
ERP Analyst	
ERP Business/Architectural Specialist	
Financial Analyst	
GIS Analyst/Programmer	
Graphics Specialist	
Groupware Specialist	
Hardware Engineer	
Hardware Engineer (Entry Level)	
Hardware Engineer (Journeyman)	
Hardware Engineer (Senior)	
Hardware Engineer (Master)	
Helpdesk Specialist	
Helpdesk Specialist (Entry Level)	
Helpdesk Specialist (Journeyman)	
Helpdesk Specialist (Senior)	
Information Assurance/Security Specialist	
Information Assurance/Security Specialist (Entry Level)	
Information Assurance/Security Specialist (Journeyman)	
Information Assurance/Security Specialist (Senior)	
Information Assurance/Security Specialist (Master)	
Information Specialist/Knowledge Engineer	
Modeling and Simulation Specialist	
Network Specialist	
Network Specialist (Entry Level)	
Network Specialist (Journeyman)	
Network Specialist (Senior)	
Network Specialist (Master)	
Program Manager	
Project Manager	

Quality Assurance Specialist							
Quality Assurance Specialist (Entry Level)	(b) (4) (b) (3)						
Quality Assurance Specialist (Journeyman)							
Quality Assurance Specialist (Senior)							
Quality Assurance Specialist (Master)							
Research Analyst							
Strategic/Capital Planner							
Subject Matter Expert							
Subject Matter Expert (Journeyman)							
Subject Matter Expert (Senior)							
Subject Matter Expert (Master)							
Systems Engineer							
Technical Editor							
Technical Writer							
Test Engineer							
Test Engineer (Entry Level)							
Test Engineer (Journeyman)							
Test Engineer (Senior)							
Training Specialist							
Training Specialist (Entry Level)							
Training Specialist (Journeyman)							
Training Specialist (Senior)							
Voice/Data Communications Engineer							
Voice/Data Communications Engineer (Entry Level)	(b) (4) (b) (3)						
Voice/Data Communications Engineer (Journeyman)							
Voice/Data Communications Engineer (Senior)							
Voice/Data Communications Engineer (Master)							
Web Content Analyst							
Web Designer							
Warehouse Technician							

B.9 INCREMENTAL FUNDING

B.9.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding for CLINs **0008A, 0008B, 0008C, 0008D, 0008E, 0009A, 0009B, 0009C, 0009D, 0010, 1002A, 1002B, 1003A, 1003B, 1004A, 1004B, 2002A, 2002B, 2003A, 2003B, 2004A, 2004B, 4005 , 4006, 0007, 1007, 2007, 3007, 3010, 4007, 4007, 9002A, 9002B, 9002C, 9003A, 9003B, 9003C, 9008A, 9008B, 9008C, 6001A, 6001B, 0009E, 6007, and 6011** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be

allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **May 30, 2018**, unless otherwise noted in Section B.7 of the Task Order. The Task Order will be modified to add funds incrementally up to the maximum of $**858, 815,756** over the performance period of this Task Order. These allotments constitute the estimated cost for the purpose of FAR Clause 52.232-22, Limitation of Funds, which applies to this Task Order on a CLIN-by-CLIN basis.

Funding Table

The funding table is located at Attachment TT

This page is intentionally left blank

B.10 AWARD FEE CALCULATION TABLE

Award Fee – Phase 1					
Period	#	Months Covered	Available Award Fee Pool	Earned Fee	Unearned Fee
Phase 1	1	CLIN 1002/3 Start + 6 Months	(b) (4) (b) (3)		
Phase 1	2	Period 1 + 6 Months			
Phase 1	3	Period 2 + 6 Months			
Phase 1	4	Period 3 + 6 Months			

Award Fee – Phase 1, Task 2				
Period	Months Covered / CLIN	Available Award Fee Pool	Earned Fee	Unearned Fee
5	6 June 2013 to 31 December 2013	(b) (4) (b) (3)		
5	CLIN 1002A			
5	CLIN 1002B			
6	1 January 2014 to 5 June 2014			
6	CLIN 1002A			
6	CLIN 1002B			
7	6 June 2014 to 31 December 2014			
7	CLIN 1002A			
7	CLIN 1002B			
8	1 January 2015 to 5 June 2015			
8	CLIN 1002B			

Award Fee – Phase 1, Task 3				
Period	Months Covered	Available Award Fee Pool	Earned Fee	Unearned Fee
5	6 June 2013 to 31 December 2013	(b) (4) (b) (3)		
5	CLIN 1003A			
5	CLIN 1003B			
6	1 January 2014 to 5 June 2014			
6	CLIN 1003A			
6	CLIN 1003B			
7	6 June 2014 to 31 December 2014			
7	CLIN 1003A			
7	CLIN 1003B			
8	1 January 2015 to 5 June 2015			
8	CLIN 1003B			

Award Fee – Phase 1, Task 4				
Period	Months Covered	Available Award Fee Pool	Earned Fee	Unearned Fee
5	22 July 2013 to 31 December 2013	(b) (4) (b) (3)		
5	CLIN 1004A			
6	1 January 2014 to 21 July 2014			
6	CLIN 1004A			
7	22 July 2014 to 31 December 2014			
7	CLIN 1004B			
8	1 January 2015 to 5 June 2015			
8	CLIN 1004B			

Award Fee – Post Phase 1, Task 2				
Period	Months Covered / CLIN	Available Award Fee Pool	Earned Fee	Unearned Fee
9	6 June 2015 to 5 December 2015	(b) (4) (b) (3)		
9	CLIN 1002B			
9	CLIN 2002A			
10	6 December 2015 to 5 June 2016			
11	6 June 2016 to 5 December 2016			
11	CLIN 2002B			
12	6 December 2016 to 5 June 2017			
12	CLIN 2002B			
12	CLIN 9002B			
13	6 June 2017 to 5 December 2017			
14	6 December 2017 to 5 June 2018			

Award Fee – Post Phase 1, Task 3				
Period	Months Covered / CLIN	Available Award Fee Pool	Earned Fee	Unearned Fee
9	6 June 2015 to 5 December 2015	(b) (4) (b) (3)		
9	CLIN 2003A			
10	6 December 2015 to 5 June 2016			
11	6 June 2016 to 5 December 2016			
11	CLIN 2003B			
12	6 December 2016 to 5 June 2017			
12	CLIN 2003B			
12	CLIN 9003A			

13	6 June 2017 to 5 December 2017	(b) (4) (b) (3) [redacted]
14	6 December 2017 to 5 June 2018	

Award Fee – Post Phase 1, Task 4				
Period	Months Covered / CLIN	Available Award Fee Pool	Earned Fee	Unearned Fee
9	6 June 2015 to 5 December 2015	(b) (4) (b) (3)		
9	CLIN 1004B			
9	CLIN 2004A			
10	6 December 2015 to 5 June 2016			
11	6 June 2016 to 5 December 2016			
11	CLIN 2004B			
12	6 December 2016 to 5 June 2017			
12	CLIN 2004B			
13	6 June 2017 to 5 December 2017			
14	6 December 2017 to 5 June 2018			

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section C of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference.

C.1 BACKGROUND

The U.S. Department of Homeland Security (DHS) is consolidating key leadership, policy, program management, and mission execution personnel on the St. Elizabeths Campus. The U.S. General Services Administration (GSA) Public Building Service (PBS) is managing all construction for St. Elizabeths for DHS.

Twenty-eight (28) DHS Component Agencies will be part of the consolidation. DHS intent is to move approximately 14,000 DHS employees onto the Campus. The consolidation will include the following DHS Components:

- DHS Headquarters, Mission Support Components, and Liaisons
  - DHS Domestic Nuclear Detection Office (DNDO)
  - DHS Science and Technology Directorate (S&T)
- U.S. Coast Guard Headquarters (USCG)
- U.S. Customs and Border Patrol Headquarters (CBP)
- Federal Emergency Management Agency Headquarters (FEMA)
- Immigration and Customs Enforcement Headquarters (ICE)
- Transportation Security Administration Headquarters (TSA)
- U.S. Secret Service (USSS)
- U.S. Citizenship and Immigration Service (USCIS)

St. Elizabeths is a National Historic Landmark (NHL) and former mental hospital that was previously operated by the Department of Health and Human Services (HHS). The West Campus and the North Parcel of the East Campus will house DHS operational needs for their IT requirements.

The West Campus, a 176-acre site, contains 62 historic buildings, 134 character-defining landscape features, and a historic cemetery in which soldiers from the Civil War era, as well as former patients, were interred. The North Parcel of the East Campus consists of approximately 23 acres.

The West Campus and the North Parcel of the East Campus will be designed to a full Interagency Security Committee (ISC) Facility Document Level 5 designation. The two (2) Campuses will be connected via an underground Campus connector for pedestrians, utilities, and infrastructure.

The St. Elizabeths construction program consists of 4.5 million gross square feet (gsf) of space including new construction and adaptive reuse of existing buildings and 1.5 million gsf of vehicular parking space nested within four (4) new garages. Subject to funding, the phasing of the project is described below:

Phase 1 consists of USCG Headquarters and USCG Command Center/Shared Use Spaces

Post Phase 1consists of Center Building, Center Building Complex, DHS HQ, Mission Support Components, DHS Operations Centers,(DOC), FEMA Headquarters, DHS Amenity Spaces, TSA, CBP, ICE, USCIS, S&T, USSS, and DNDO

GSA PBS has awarded a construction contract to Clark Construction (Clark) for Phase 1 construction of the USCG HQ. Clark has incorporated pathways for vertical fiber, horizontal copper, and ladder racks as a place holder in the design document. There are no active elements of the required local area network (LAN) or other telecom equipment included. GSA will be executing other contracts for new construction and adaptive reuse for Post Phase 1.

The TIP Contractor shall validate and utilize to the maximum extent possible construction and bridging designs provided by the government which address IT outside plant duct systems, building cabling pathways, physical security system infrastructure, and utility pathways. These designs will be provided after award, specifically address Phase 1 requirements and shall be considered prior to execution of this task.

GSA awarded Parsons a separate contract for a Campus Coordinator. The Campus Coordinator is the "Master Scheduler," and will be responsible for integrating the schedules of all Contractors working on the construction program (Architects and Engineers, Construction, Information Technology, and Furniture/Fixtures) into the Master Schedule. The TIP Contractor shall coordinate all activities with the Campus Coordinator.

C.2 SCOPE OF WORK

GSA PBS is utilizing GSA Federal Acquisition Service (FAS) Assisted Acquisition Service (AAS) support to award and manage an integration Contractor to design, procure, configure/install, test, secure, accredit, and maintain a seamless, integrated transport infrastructure. The scope of DHS TIP is to create a physically and logically diverse and redundant Campus infrastructure that will support everything on and within the perimeter fence. Open System Interconnection Reference Model (OSI Reference Model or OSI Model) Layer 1 - Physical Layer and Layer 2 - Data-Link Layer are included in their entirety for the Campus. Aspects of Layer 3 - Network Layer are partially included, as are higher layers for on-site specialized systems (e.g., security, smart buildings applications, and fire safety systems.)

C.3 OBJECTIVES

The DHS mission is to lead a unified national effort to secure America. DHS legacy facilities are dispersed over more than 60 buildings throughout the National Capital Region (NCR), some with sub-optimal security protections and routinely adversely impacting critical communication, coordination, and cooperation across DHS Components. To support the incident management and command-and-control requirements of this mission, DHS has a clear need to consolidate executive leadership and operational management in a secure setting. This will foster a "one DHS" culture and optimize prevention and response capabilities across the spectrum of

operations. DHS also needs to significantly reduce the total number of locations that house DHS Components to as few as possible to lower overall costs.

DHS views the St. Elizabeths Campus as a single integrated entity. The Campus will not be Component-specific, and individual Components residing on the Campus will become part of the integrated fabric. None of the Components are moving their entire operations onto the Campus. The portion of each Component that does not move will continue to maintain its own off Campus IT infrastructure, support structure, and help desks. Support for these operations is outside the scope of DHS TIP; however, close coordination with these support groups shall be required both during transition and Operations & Maintenance (O&M) to assure seamless support to the end users. Business continuity and mission support during the consolidation effort is essential.

DHS recognizes the importance of using distributed renewable energy generation to meet mission needs at facilities, to reduce operational costs and minimize exposure to price fluctuations, to improve reliability, and to reduce greenhouse gas emissions. The TIP Contractor shall consider the reduction of energy consumption on-Campus in the design and operations, as well as the potential for increased use of renewable energy. The TIP Contractor shall identify opportunities to implement renewable and distributed energy generation technologies, and shall analyze the associated risks and benefits of each.

The following technical objectives apply to DHS TIP infrastructure and systems:

- Open Standards
- Everything over IP (EOP)
- Power Over Ethernet (POE) end devices for IT, physical security and IBS components
- Implementation of Joint Interoperability Test Command (JITC) certified equipment, technology, and solutions where applicable
- Internet Protocol version 6 (IPV6) capable
- Energy efficient IT solutions and infrastructure
- Pathway efficient cabling solutions
- Passive Optical Networking (PON) utilization

Deviations from these objectives may benefit the government in certain functional areas and will be evaluated on a case-by-case basis.

C.4 TASKS

C.4.1 Task 1 – PROVIDE Program Management

The TIP Contractor shall provide program management support under this Task Order. This includes the management and oversight of all activities performed by TIP Contractor personnel, including subcontractors, to satisfy the requirements identified in this Task Order. The TIP Contractor shall identify a Program Manager (PM) by name, which shall provide management, direction, administration, quality assurance, and leadership of the execution of this Task Order.

C.4.1.1 SUBTASK 1 – COORDINATE A PROJECT KICKOFF MEETING

The TIP Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location specified by the Government. The meeting will provide an introduction between the TIP Contractor personnel and Government personnel who will be involved with the Task Order. The meeting will provide the opportunity to discuss technical, management, security issues, travel authorization, and reporting procedures. At a minimum, the attendees shall include all vital TIP Contractor personnel, representatives from the affected Components, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR). The TIP Contractor shall provide the following at the Kick-Off Meeting:

- Program Management Plan
  - Work Breakdown Structure (WBS)
  - Quality Management Plan (QMP)
  - Earned Value Management Plan (EVMP)
  - Risk Management Plan (RMP)
  - Configuration Management Plan (CMP)

C.4.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor Program Manager shall develop and provide a Monthly Status Report (MSR) using MS Office Professional 2010 software applications, by the 10th business day of each month via electronic mail to the Technical Point of Contact (TPOC) and Contracting Officer's Representative (COR). The MSR shall include the following:

- Activities during reporting period, by task (e.g., on-going activities, new activities, activities completed; progress to date on all above mentioned activities)
- Service Level Agreement (SLA) and Metrics Monthly Report to include issues, concerns, and proposed resolutions for missed SLA's and metrics
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them
- Personnel gains, losses and status, security clearance adjudication, etc.
- Government actions required
- Schedule - major tasks, milestones, and deliverables; planned and actual start and completion dates for each
- Accumulated invoiced cost for each CLIN up to the previous month
- Projected cost of each CLIN for the current month

C.4.1.3 SUBTASK 3 - EARNED VALUE MANAGEMENT (EVM) CRITERIA

The TIP Contractor shall employ and report on Earned Value Management (EVM) in the management of this Task Order.

The TIP Contractor shall employ EVM in the management of this Task Order in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, Earned Value Management Systems. The Standard-748-B-2007 is also permissible. The TIP Contractor shall employ EVM techniques in accordance with industry best practices. EVM only applies to CPAF and CPFF CLINS. The following EVM status information shall be included in each Monthly Status Report:

- Planned Value (PV)
- Earned Value (EV)
- Actual Cost (AC)
- A cost curve graph plotting PV, EV, and AC on a monthly basis from inception of the Task Order through the last report, and plotting the AC curve to the estimated cost at completion (EAC) value
- An EVM variance analysis that includes the following:
  - Cost Variance (CV) = (EV - AC)
  - Cost Variance % = (CV/PV X 100%)
  - Cost Performance Index (CPI) = (EV/AC)
  - Schedule Variance (SV) = (EV minus PV)
  - Schedule Variance % = (SV/PV X 100%)
  - Schedule Performance Index (SPI) = (EV/PV)
  - Estimate at Completion (EAC)
  - ACcum + 1/CPI X (BAC minus EV cum)
  - ACcum + 1/CPI X SPI X (BAC minus EV cum)
  - Variance at Completion (VAC) = (BAC minus EAC) for EAC
  - Variance at Completion % + (VAC/BAC X 100%) for EAC
  - Estimate to Completion (ETC)
  - Expected Completion Date
- Explain all Current Period variances greater than both +/-10% **and** $10k.
- Explain all Cumulative period variances greater than both +/-10% **and** $50k.
- Explain all Variance at Completion variances greater than both +/-10% **and** $100k.
- Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved
- Discuss the corrective actions that will be taken to correct the variances, and the risks associated with the actions

The Monthly Reporting Deliverables provided by DHS TIP will be as follows:

- Integrated Master Schedule (MS Project 2010)
- CPR FORMAT 1 (at Control Account level)
- CPR FORMAT 3 (at Control Account level)
- CPR FORMAT 5 (at Control Account level)
- Monthly Insight integration file. (at Control Account level)

These monthly deliverables will be due to the Government by the fifteenth (15^{th}) business day after the close of the Fiscal Month.

The Government will conduct an Integrated Baseline Review within 145calendar days after Task Order award, and 90 calendar days after the exercise of significant Task Order options or the incorporation of major Task Order modifications. The objective of the Integrated Baseline Review is for the Government and the TIP Contractor to jointly assess areas, such as the TIP Contractor's planning, to ensure complete coverage of this Task Order, logical scheduling of the work activities, adequate resources, and identification of inherent risks.

C.4.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The TIP Contractor Program Manager shall convene technical status meetings with the TPOC and/or COR, and other Government stakeholders as necessary. The purpose of these meetings is to ensure all stakeholders are informed of the activity and status, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The TIP Contractor Program Manager shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the TPOC and COR within five (5) calendar days following the meeting.

C.4.1.5 SUBTASK 5 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The TIP Contractor shall document all support requirements in a Program Management Plan (PMP). The PMP shall:

- Describe the proposed management approach
- Reference detailed Standard Operating Procedures (SOPs) for all mandatory and exercised optional tasks
- Include milestones, tasks, and subtasks required in this Task Order
- Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations
- Include the TIP Contractor’s QMP, CMP, and EVM Plan
- Describe the overall approach to mitigating risk at the program and individual project level in a Risk Management Plan
- Provide detailed project management task information (prescribed in C.4.4.5.2.5)

The TIP Contractor shall provide the Government with a draft PMP, on which the Government will make comment. The final PMP shall incorporate Government comments.

C.4.1.6 SUBTASK 6 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP) AND QUALITY MANAGEMENT PLAN (QMP)

The PMP and Quality Management Plan (QMP) are evolutionary documents that shall be updated annually. The TIP Contractor shall work from the latest Government-approved versions of each document.

C.4.1.7 SUBTASK 7 – DEVELOP TRAINING PLAN

Upon the exercise of Task 4 for Phase 1, the TIP Contractor shall develop a training plan to implement the training requirements in Task 4.

C.4.1.8 SUBTASK 8 – CHANGE MANAGEMENT

The TIP Contractor shall manage the Change Management process in accordance with the DHS Governance and Infrastructure Change Control Board as described in Attachment B. The TIP Contractor shall perform change management activities in conformance with the most recent version of Information Technology Infrastructure Library (ITIL) guidelines. The TIP Contractor will provide detailed Configuration Management Plan and Configuration Management DataBase (CMDB) information after Task Order award. The TIP Contractor shall comply with the DHS Change Management requirements for all equipment, hardware, system software, applications software (both source and executable), data files, and control-language.

C.4.1.9 SUBTASK 9 – COORDINATION WITH OTHER CONTRACTORS

The TIP Contractor shall coordinate with Government and third-party contractor personnel performing required services in areas associated with the requirements of this Task Order. Some examples of the required services are personnel performing security and continuity functions, audits, inspections, independent verification & validation, delivery services, construction, and telecommunication services.

The TIP Contractor shall utilize a Government provided Enterprise electronic Project Management (e-PM) system on this project. e-PM is defined as an internet-based information and project communication system that allows the St. Elizabeths project team (e.g., GSA PBS, GSA FEDSIM, DHS, all construction contractors) to collaborate in a centralized and secured repository. All DHS TIP project-specific correspondence for Tasks 1, 2, and 3 (e.g., during the construction phases, not during operations & maintenance post occupancy of each phase), workflow processes, and documentation that will affect Other Government Contractors (OGC) on the St Elizabeths project will be stored and routed within the ePM system.

The ePM system is based on the Proliance software that was developed by Meridian Systems. Users will be provided a username and password after they have completed the HSPD-12 process. The TIP Contractor shall log into the e-PM system to enter the Project Documentation listed in the bulleted list below.

GSA PBS will hold several training sessions to familiarize relevant TIP Contractor staff (e.g, project control personnel).

In accordance with Section F.5 Deliverables, the TIP Contractor shall post, store, and maintain all deliverables and all documentation produced pursuant to this Task Order on the contractor-provided DHS TIP SharePoint Portal.

In addition, the TIP Contractor is required to timely and accurately post, review, respond, and collaborate with OGCs using the following features and/or workflow processes within the ePM system:

- Project Team Directory – The TIP Contractor shall provide an updated directory of contact information for all companies, subcontractors and project team members who are engaged on this project.
- Schedules – The TIP Contractor shall post, review, and/or respond to Critical Path Method schedule updates within the ePM system and shall receive schedule updates from OGCs.
- Design Drawings/Design Packages – The TIP Contractor shall submit design drawings and design packages into the system and receive design drawings and design packages from OGCs.
- Punchlists – Maintain list(s) of observed defects and omissions.
- Issue Tracking – The TIP Contractor to log and respond to issues that are related and affect OGCs.
- Requests for Information (RFI) – The TIP Contractor will enter Requests for Information from OGCs into the system and will respond to RFIs from OGCs in the system.

The COR or TPOC will facilitate initial contact between the TIP Contractor and other third-party contractors performing work for DHS. The TIP Contractor shall provide support services to other third-party contractors within the scope of this Task Order as required by the Government. The TIP Contractor shall notify the designated representative in writing of unresolved disputes in receiving support from or providing support to customers or other third-party contractors within two (2) business days from the time the dispute occurs.

C.4.1.10 SUBTASK 10 – RISK MANAGEMENT

DHS TIP requires a systematic structured, formalized, forward thinking, and continuous approach to risk management at the program and project level. The Risk Management Program shall be a value-based systematic approach to managing all risks from all sources to improve the TIP Contractor's performance in meeting the objectives of DHS TIP. The TIP Contractor shall use the best commercial and Government practices to develop, implement, and manage, on an ongoing basis, the Risk Management Program for DHS TIP. The risk management process shall be flexible and adaptable. The Risk Management Program (included in the Program Management Plan) shall provide clear visibility into program risks in the areas such as, but not limited to scope costs, schedule, and technical performance. The Risk Management Program should also account for risks at the subcontractor level. The TIP Contractor shall be responsible for utilizing a commercial-off-the-shelf (COTS) software for use in managing the risk process. A feedback system shall also be in place for project managers to easily make comments and suggestions for improvements to materials and the process. At a minimum, The TIP Contractor shall track risks, risk levels, operate a risk management database, and report at monthly status meetings on risks and mitigations.

C.4.1.11 SUBTASK 11 – QUALITY MANAGEMENT

The TIP Contractor shall update the Quality Management Plan (QMP) submitted with their proposal and provide a final QMP as shown in Section F. The QMP plays an important role in

ensuring the TIP Contractor meets the contract requirements and the quality expectations of the Government. The TIP Contractor shall be responsible for establishing the infrastructure, support organizations, processes, tools and procedures to implement the QMP. The QMP shall describe the quality management system.

The QMP shall describe the quality assurance procedures, quality control activities and other technical activities to be implemented.

C.4.1.12 SUBTASK 12 – SUPPORT DHS WORKING CAPITAL FUND

The TIP Contractor shall support the DHS Cost Model and Delivery of subscription services (e.g., subscription services based billing sensitivity, identify utilization of specific resources to so specific component organizations, allowing for reporting a level of detail to the Working Capital Fund (WCF) billing services necessary to justify billing rates). The TIP Contractor shall support this type of billing environment through cost and resource tracking for Tasks 4, 5, 6, and 7.

Note: Task 4 – The WBS for operations and maintenance is aligned with the DHS Working Capital Fund. The TIP Contractor shall collect costs in support of DHS WCF billing methodology.

C.4.1.13 SUBTASK 13 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

C.4.1.14 SUBTASK 14 – WORKFLOW & DATABASE

The TIP Contractor shall support all contractual consent to purchase and travel requests through a contractor provided web based workflow application. The system shall support file attachments, provide a means of authentication, and store all DHS TIP task order requests.

C.4.1.15 SUBTASK 15 – PROVIDE PROGRAM MANAGEMENT-POST PHASE 1

The TIP Contractor shall provide program management support under this Task Order during Post Phase 1. This includes the management and oversight of all activities performed by TIP Contractor personnel, including subcontractors, to satisfy the requirements of the task order and planned activities during Post Phase 1. Examples could include Post Phase 1 Program Planning, Reporting, Documentation Support, SharePoint Portal Access/Maintenance, Phase 1 Transition-out, Facilities (Warehouse, Trailers, Offices) Decommissioning, and Ad-hoc Reporting.

C.4.1.15.1 PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor Program Manager shall develop and provide a Monthly Status Report (MSR) using MS Office Professional 2010 software applications, by the 10th business day of each month via electronic mail to the TPOC and Contracting Officer's Representative (COR). The MSR shall include the following:

- Activities during reporting period, by task (e.g., on-going activities, new activities, activities completed; progress to date on all above mentioned activities)
- Service Level Agreement (SLA) and Metrics Monthly Report to include issues, concerns, and proposed resolutions for missed SLA's and metrics
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them
- Personnel gains, losses and status, security clearance adjudication, etc.
- Government actions required
- Schedule - major tasks, milestones, and deliverables; planned and actual start and completion dates for each
- Accumulated invoiced cost for each CLIN up to the previous month
- Projected cost of each CLIN for the current month

The MSR may be delivered electronically and an in-person presentation of the report will not be required.

C.4.1.15.2 EARNED VALUE MANAGEMENT (EVM) CRITERIA

The TIP Contractor shall employ and report on Earned Value Management (EVM) in the management of this Task Order.

The TIP Contractor shall employ EVM in the management of this Task Order in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, Earned Value Management Systems. The Standard-748-B-2007 is also permissible. The TIP Contractor shall employ EVM techniques in accordance with industry best practices. EVM only applies to CPAF and CPFF CLINS. The following EVM status information shall be included in each Monthly Status Report:

- Planned Value (PV)
- Earned Value (EV)
- Actual Cost (AC)
- A cost curve graph plotting PV, EV, and AC on a monthly basis from inception of the Task Order through the last report, and plotting the AC curve to the estimated cost at completion (EAC) value
- An EVM variance analysis that includes the following:
  - Cost Variance (CV) = (EV - AC)
  - Cost Variance % = (CV/PV X 100%)
  - Cost Performance Index (CPI) = (EV/AC)
  - Schedule Variance (SV) = (EV minus PV)
  - Schedule Variance % = (SV/PV X 100%)

  - Schedule Performance Index (SPI) = (EV/PV)
  - Estimate at Completion (EAC)
  - ACcum + 1/CPI X (BAC minus EV cum)
  - ACcum + 1/CPI X SPI X (BAC minus EV cum)
  - Variance at Completion (VAC) = (BAC minus EAC) for EAC
  - Variance at Completion % + (VAC/BAC X 100%) for EAC
  - Estimate to Completion (ETC)
  - Expected Completion Date
- Explain all Current Period variances greater than both +/-10% **and** $10k.
- Explain all Cumulative period variances greater than both +/-10% **and** $50k.
- Explain all Variance at Completion variances greater than both +/-10% **and** $100k.
- Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved
- Discuss the corrective actions that will be taken to correct the variances, and the risks associated with the actions

The Monthly Reporting Deliverables provided by DHS TIP will be as follows:

- Integrated Master Schedule (MS Project 2010)
- CPR FORMAT 1 (at Control Account level)
- CPR FORMAT 3 (at Control Account level)
- CPR FORMAT 5 (at Control Account level)
- Monthly Insight integration file. (at Control Account level)

These monthly deliverables will be due to the Government by the fifteenth (15^{th}) business day after the close of the Fiscal Month. This deliverable will be required during CLIN 2001 Option Year 2 until Phase 1 Tenant Move-In and EVM activities are closed out.

C.4.1.15.2 CONVENE TECHNICAL STATUS MEETINGS

The TIP Contractor Program Manager shall convene technical status meetings with the TPOC and/or COR, and other Government stakeholders as deemed necessary by the government. The purpose of these meetings is to ensure all stakeholders are informed of the activity and status, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The TIP Contractor Program Manager shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the TPOC and COR within five (5) calendar days following the meeting.

C.4.1.15.3 PHASE 1 CHANGE MANAGEMENT

During Post Phase 1, the TIP Contractor shall manage the Change Management process for Phase 1 activities through scheduled completion in accordance with the DHS Governance and

Infrastructure Change Control Board as described in Attachment B. The TIP Contractor shall perform change management activities in conformance with the most recent version of Information Technology Infrastructure Library (ITIL) guidelines. The TIP Contractor shall comply with the DHS Change Management requirements for all equipment, hardware, system software, applications software (both source and executable), data files, and control-language.

C.4.1.15.4 COORDINATION WITH OTHER CONTRACTORS

The TIP Contractor shall coordinate with Government and third-party contractor personnel performing required services in areas associated with the requirements of this Task Order during Post Phase 1. Some examples of the required services are personnel performing security and continuity functions, audits, inspections, independent verification & validation, delivery services, construction, telecommunication services, and USCG help desk and support contractors.

The TIP Contractor shall utilize a Government provided Enterprise electronic Project Management (e-PM) system on this project. e-PM is defined as an internet-based information and project communication system that allows the St. Elizabeths project team (e.g., GSA PBS, GSA FEDSIM, DHS, all construction contractors) to collaborate in a centralized and secured repository. All DHS TIP project-specific correspondence for Tasks 1, 2, and 3 workflow processes, and documentation that will affect OGCs on the St Elizabeths project will be stored and routed within the ePM system.

The ePM system is based on the Proliance software that was developed by Meridian Systems. Users will be provided a username and password after they have completed the HSPD-12 process. The TIP Contractor shall log into the e-PM system to enter the Project Documentation listed in the bulleted list below.

In accordance with Section F.5 Deliverables, the TIP Contractor shall post, store, and maintain all deliverables and all documentation produced pursuant to this Task Order on the contractor-provided DHS TIP SharePoint Portal.

In addition, the TIP Contractor is required to timely and accurately post, review, respond, and collaborate with OGCs using the following features and/or workflow processes within the ePM system:

- Project Team Directory – The TIP Contractor shall provide an updated directory of contact information for all companies, subcontractors and project team members who are engaged on this project.
- Schedules – The TIP Contractor shall post, review, and/or respond to Critical Path Method schedule updates within the ePM system and shall receive schedule updates from OGCs.
- Design Drawings/Design Packages – The TIP Contractor shall submit design drawings and design packages into the system and receive design drawings and design packages from OGCs.
- Punchlists – Maintain list(s) of observed defects and omissions.

- Issue Tracking – The TIP Contractor to log and respond to issues that are related and affect OGCs.
- Requests for Information (RFI) – The TIP Contractor will enter Requests for Information from OGCs into the system and will respond to RFIs from OGCs in the system.

The COR or TPOC will facilitate initial contact between the TIP Contractor and other third-party contractors performing work for DHS. The TIP Contractor shall provide support services to other third-party contractors within the scope of this Task Order as required by the Government. The TIP Contractor shall notify the designated representative in writing of unresolved disputes in receiving support from or providing support to customers or other third-party contractors within two (2) business days from the time the dispute occurs.

C.4.1.15.5 RISK MANAGEMENT

DHS TIP requires a systematic structured, formalized, forward thinking, and continuous approach to risk management at the program and project level. The Risk Management Program shall be a value-based systematic approach to managing all risks from all sources to improve the TIP Contractor's performance in meeting the objectives of DHS TIP. The TIP Contractor shall use the best commercial and Government practices to develop, implement, and manage, on an ongoing basis, the Risk Management Program for DHS TIP. The risk management process shall be flexible and adaptable. The Risk Management Program (included in the Program Management Plan) shall provide clear visibility into program risks in the areas such as, but not limited to scope costs, schedule, and technical performance. The Risk Management Program should also account for risks at the subcontractor level. The TIP Contractor shall be responsible for utilizing a commercial-off-the-shelf (COTS) software for use in managing the risk process. A feedback system shall also be in place for project managers to easily make comments and suggestions for improvements to materials and the process. At a minimum, The TIP Contractor shall track risks, risk levels, operate a risk management database, and report at monthly status meetings on risks and mitigations.

C.4.1.15.6 WORKFLOW & DATABASE

The TIP Contractor shall support all contractual consent to purchase and travel requests through a contractor provided web based workflow application. The system shall support file attachments, provide a means of authentication, and store all DHS TIP task order requests.

C.4.2 Task 2 – PROVIDE REQUIREMENTS ANALYSIS AND DESIGN

The TIP Contractor shall collect, refine, validate, and analyze IT, physical security, and IBS requirements for optimal quality, cost, and compliance. The TIP Contractor shall develop detailed designs integrating key technologies and systems over a common Campus network infrastructure.

Historically, Government building and Campus physical security systems and infrastructure have been kept physically separate from IT data network infrastructure. This was primarily a result of

policy; however difference in system availability requirements, network technologies and protocols, bandwidth requirements and O&M and security issues also contributed to this separation. As the St. Elizabeths campus infrastructure is being designed to address these concerns; high availability, non-blocking, community of interest (COI) logically separated networks, secure, scalable and flexible P-OTP campus fabric, combined with the convergence of IP and Ethernet enabled physical security system end-points, it may be possible to leverage the Campus infrastructure to transport the physical security information while meeting all the requirements set forth by DHS and government physical security policy and guidance. The TIP Contractor shall recommend the extent by which the physical security systems should utilize the Campus infrastructure to meet all the requirements set forth in the ISC Physical Security Criteria for Federal Facilities level 5 descriptions (provided in Attachment C).

The TIP Contractor shall comply with DHS policies, standards, and procedures as they relate to this Task Order. When technologies do not comply with current standards the TIP Contractor shall comply with all policies and procedures for the introduction of new technologies per the authorization to operate (ATO), Technical Refresh Model (TRM), Infrastructure Change Control Board (ICCB), and Certification and Authorization (C&A) processes. All compliance must comply with the following:

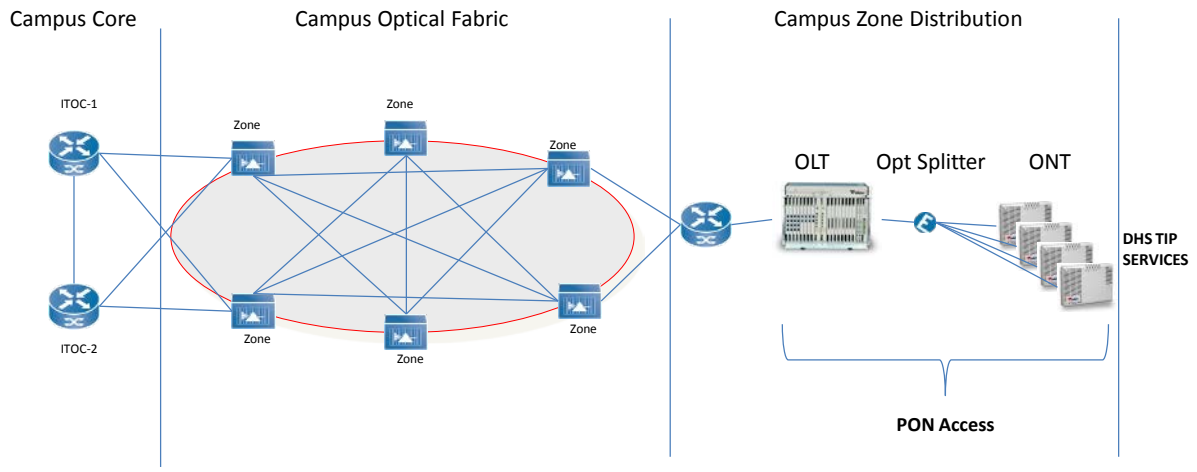
- All developed solutions and requirements shall comply with the Homeland Security Enterprise Architecture (HLSEA)
- All IT hardware or software shall comply with the HLSEA Technical Reference Model (TRM) Standards and Products Profile as described in Attachment D
- The TIP Contractor shall submit all data assets, information exchanges and data standards, whether adopted or developed to the DHS MGMT/OCIO/ITSO/Enterprise Data Management Office (EDMO) through the ITSO/CRMD/St. Elizabeth Special Program Office for review and insertion into the DHS Data Reference Model

C.4.2.1 SUBTASK 1 – INFORMATION TECHNOLGOY

C.4.2.1.1 INFRASTRUCTURE

The TIP Contractor shall design the campus infrastructure to provide secure, reliable, and efficient transport for network and system voice, video, and data traffic.

The campus infrastructure will be divided into three (3) primary campus network layers: access, distribution, and core as shown below:



The building Access Layer transport will utilize Passive Optical Network (PON) technology and service the end devices on campus. The Distribution Layer, broken out and referred to as "Zones" on the Campus, will aggregate all the building PONs based on density of end items, geography of the campus, and the chronologically-phased approach of the construction effort. The Core Layer, which will perform high speed routing, switching, and network security functions will be located in the campus Information Technology Operations Center ITOC-1 and ITOC-2. Interconnecting the Zones to the core nodes and to the demarcation points will be the DHS Campus fabric using optical technologies such as packet optical transport platform (P-OTP), Optical Transport Network (OTN) and dense wavelength division multiplexing (DWDM). The Core layer, Distribution Layer, Campus fabric, and portions of the access layer will be designed to meet the High Availability requirements set forth in the most recent version of the Department of Defense (DoD) Unified Capabilities Requirements (UCR) document. The infrastructure will provide Community of Interest (COI) separation capability. A COI can be a logical and/or physical grouping of network devices or users with access to information that should not be made available to the general user population on a LAN or WAN infrastructure. A COI will be utilized to provide multiple levels of protection for the LAN and/or WAN infrastructure from the activities within the COI. A COI may consist of a logical perimeter around the community (or enclave), and may allow for separate security management and operational direction. A COI will not dictate separate internal security policies (e.g., password

policies, etc.) because that will fall under the jurisdiction and management of DHS. However, a COI may have a subset of overall network security policy.

The Campus infrastructure architecture is designed to meet DHS TIP objectives in Section C.3. The TIP Contractor may propose alternative designs, technologies and solutions which improve upon the proposed architecture in order to meet or exceed TIP objectives.

C.4.2.1.1.1 Campus and Building Wiring

The TIP Contractor shall design and install all Campus wiring between buildings, within new and adaptive reuse buildings, transitioning through utility tunnels, connecting to the central utility plant (CUP), and to include perimeter security. Asbestos abatement is outside the scope of the DHS TIP. Campus inside and outside plant pathway designs for Phase 1 will be developed prior to award of this contract. The TIP Contractor shall be required to review, analyze, and use existing designs developed during the GSA bridging activities.

There will be non-DHS tenants on the Campus (e.g., credit union, dry cleaners, food service, fitness center, child care centers, barber, etc.) that will require phone and data access external to the Campus. These services will be paid for by those tenants, but must utilize the combined infrastructure while maintaining IT and communications security separation from other DHS COIs. These facilities are within the scope of the DHS TIP.

Utility tunnels already exist on the Campus. Additional tunnels have been designed and will be built as part of the Construction Contract. All fiber will be run through the tunnels and, where necessary, in “direct burial” fiber/cable duct tubing. The GSA construction Contractors will install the conduit; the TIP Contractor shall be responsible for pulling cable/fiber through the conduit within the utility tunnels and/or direct burial paths.

The TIP Contractor shall provide input to the GSA construction Contractors on a regular basis regarding building and tunnel designs based on the IT design requirements. The TIP Contractor shall make recommendations for types of cable/fiber that will support the optical network, including PON, while providing maximum utilization in support of all technology services and requirements listed within this Task Order.

C.4.2.1.1.2 Passive Optical Network – Access Layer

A Passive Optical Network (PON) is a point-to-multipoint, fiber to the premises network architecture in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises. The DHS Campus PON will consist of an optical line terminal(s) (OLT) resident to the Campus and optical network units (ONU) located very near end devices. The TIP Contractor shall design PON primarily within the buildings as the Access Layer voice, video, and data transport. Due to the severe space limitations on Campus and the desire to be certified for Leadership in Energy and Environmental Design (LEED) Silver Level, GSA and DHS requires the use of PON technology. This may include Gigabit Passive Optical Network (GPON), Gigabit Ethernet Passive Optical Network (GEPON), and Wave Division Multiplex Passive Optical Network (WDPON or WDMPON) technology. The proposed technology should

have no active elements requiring intermediate wire closets; it should use patch panels locally rather than routers or switches; and should reduce requirements for power, cooling, heating, and floor space. The TIP Contractor shall propose the handling and transport of classified and unclassified data across PON. Consideration shall be placed on encryption, bundles, filaments, and segregation versus no segregation. This infrastructure shall support all forms of end-user services including voice, data, video, and cable TV. It is the intent that, to the greatest extent possible, all services ride the single integrated infrastructure. This may utilize virtual local area network (VLAN) separation, wavelength separation, and/or Level 1 encryption as end-user devices to accomplish this goal while meeting applicable security regulations. Specific component technical requirements will be discussed and addressed during this task. The TIP Contractor shall design PON split ratios to ensure constant and peak bandwidth delivery to end items based on end user bandwidth demands.

C.4.2.1.1.3 Zone – Distribution Layer

The TIP Contractor shall design the Zones on the Campus to aggregate the PONs based on density of end items, geography of the Campus, and chronological phased approach of the construction effort. The TIP Contractor shall consider routing and/or switching functions, traffic filtering and shaping, and Community of Interest logical and/or physical separation. The Distribution Layer shall be designed to deliver end user constant and peak bandwidth requirements in a non-blocking fashion.

C.4.2.1.1.4 Campus Fabric

The TIP Contractor shall design a robust, flexible, redundant, scalable, secure, and efficient Campus fabric to provide transport between the core nodes, buildings, Zones and the four (4) planned demarcation points on Campus. The TIP Contractor shall be required to utilize packet optical transport platform (P-OTP)/OTN and DWDM or equivalent technologies for the Campus fabric to transport the DHS analog and digital voice, video, and data. The Campus fabric shall be designed to transport and deliver end user, facilities, and equipment constant and peak bandwidth requirements in a non-blocking fashion.

C.4.2.1.1.5 Core Layer

The TIP Contractor shall design the Core Layer of the Campus infrastructure in ITOC-1 and ITOC-2. The Core Layer shall provide high-speed, non-blocking, redundant routing and switching functions for the Campus infrastructure. Also located at the core location shall be the separate network perimeter security devices for the “dot GOV .gov” and the “dot MIL .mil” networks. The ITOC facilities will be used to provide redundancy and survivability for the .gov and .mil network core.

C.4.2.1.1.6 Off-Campus Data Center Connectivity

DHS has two (2) Data Centers (DC). DC-1, also called the national Center for Critical Information Processing and Storage (NCCIPS), is a shared Government-owned facility at the John C. Stennis Space Center (SSC) in Mississippi. DC-2 is a contract data center operated in

Clarksville, Virginia. DC-1 and DC-2 are capable of mirroring each other and can support up to eight (8) levels of data recovery. Each DHS Component will choose the backup level specific to its mission needs. The TIP Contractor shall determine the requirements for each DHS Component selected backup level as part of the Task Order. Additionally, the USCG maintains connectivity with their own special "dot-MIL .mil" data center in Clarksburg, West Virginia for DoD required services and data bases. The TIP Contractor shall perform the analysis and design support for component specific Data Center connectivity requirements.

C.4.2.1.1.6.1 Demarcation Points

The point at which a telecommunications carrier network ends and the DHS Campus network begins is a demarcation point (demarc). There are four (4) demarcs distributed throughout the Campus located in vaults. Vaults are not provided by the TIP Contractor, but by the Construction Contractors. These four (4) demarcs are designed to be geographically diverse. Additionally, they are designed to be diverse and redundant to each telecommunications carrier. These shall be the only off-Campus connections to the outside other than by satellite or other forms of wireless communications systems designated as backup or redundant in nature. Connectivity to other external agencies, to DHS Components that are not resident on Campus, to the DHS Cloud (i.e., ONENET, Data Centers and server farms across the nation), and to public networks shall go through the specialized circuits at the established four demarcs. The TIP Contractor shall accommodate these telecommunication carrier circuits when designing transport to on-Campus buildings.

C.4.2.1.1.6.2 DHS ONENET

ONENET is DHS Wide-Area Network (WAN). The TIP Contractor shall coordinate with the ONENET Program Management Office (PMO) in order to determine the overall bandwidth requirements for the Campus. The TIP Contractor shall follow the DHS Authority to Operate (ATO) procedures, Certification and Accreditation (C&A), conduct proper security test and evaluation (ST&E), and use the DHS Configuration Management (CM) processes prior to being allowed to interface with DHS ONENET. Data shall be transported over the DHS ONENET to the demarcs and shall then be distributed within the Campus.

C.4.2.1.1.6.3 Remote Satellite Connectivity

The TIP Contractor shall design connectivity to external satellite feeds as required, which shall be accessed from any number of the four (4) Campus demarcs via DHS ONENET or over wired connections from the DHS Nebraska Avenue Complex (NAC) or other Government locations, and shall have to be distributed via the Campus fabric from these demarcs.

C.4.2.1.1.6.4 Defense Information Systems Network (DISN)

The TIP Contractor shall coordinate and interface with "dot MIL (.mil)" networks on Campus with DoD Defense Information Systems Network (DISN). The .mil access shall also to be provided at all demarcs.

C.4.2.1.1.7 Radio Frequency Mobility Service

The TIP Contractor shall design and provide a broad range of RF Mobility Services. The RF Mobility Service requirements shall be collected, refined, validated, and analyzed during this task. A deliverable from this task shall be a comprehensive RF Mobility Service architecture which addresses the design of an underlying radio frequency spectrum distribution infrastructure system. The RF Mobility Service shall efficiently and securely distribute multiple RF required by the overlaying mobility services, both on-Campus and within buildings. The infrastructure shall be easily upgradable, reconfigurable, and/or scalable to allow for the propagation of additional RF required by new RF Mobility Service technologies as they become available. Green efficiencies in the Mobility Service architecture and design are encouraged. The TIP Contractor's design is constrained due to the Programmatic Agreement and Section 106 of the National Historic Preservation Act (NHPA), which may limit the use, size, quantities, and locations of external and internal antennas, equipment, and other required RF Mobility Service infrastructure. The TIP Contractor must ensure RF transmitters are not placed in proximity to any Campus Sensitive Compartmented Information Facility (SCIF) or facilities processing classified information according to DHS, DoD, and Federal security policies and guidelines.

C.4.2.1.1.7.1 Mobile Wireless Communications

The TIP Contractor's design shall ensure holistic all carrier support for unclassified and classified solutions that provides in-building and campus wide mobile wireless communications. Service shall include Cellular, Personal Communications Service (PCS), Long Term Evolution (LTE), and Advanced Wireless Services (AWS). The solution shall include wireless priority and precedence support for designated personnel.

The TIP Contractor shall be responsible for the acquisition, support, and service of all Government issued mobile devices for staff assigned to the campus. This service includes coordination with existing contractors, establishment of a multi-vendor acquisition model, and asset management.

C.4.2.1.1.7.2 Land Mobile Radio (LMR)

The LMR system shall support DHS life safety, emergency, security, Continuity of Operations (COOP), and Continuity of Government (COG) requirements. The TIP Contractor shall design a LMR distribution infrastructure and system to allow required DHS LMR services to operate both on-Campus and within buildings. Various frequency ranges shall be required to support these services. The TIP Contractor shall be responsible for evaluating the needs of DHS and its subcomponents along with the land mobile radio system technologies to determine the most efficient solution. The solution shall have enhanced performance capabilities and functionality as well as have the ability to operate in both the Ultra High Frequency (UHF) and Very High Frequency (VHF) spectrums as determined by the DHS Subcomponents. The TIP Contractor shall also integrate the Emergency ("E") LMR system with DHS Component LMR systems, and with other additional local, state and Federal agency systems where required to ensure communication across systems is possible.

C.4.2.1.1.7.3 Wireless Networking Capability

C.4.2.1.1.7.3.1 Wi-Fi

The TIP Contractor shall design a DHS Wi-Fi system to meet all current IEEE 802.11 radio standards (IEEE 802.11a /b/g/n) using discrete access points (APs) provisioned with multiple, integral radio frequency antennae. The system shall have the ability to selectively restrict Campus Wi-Fi users to internet access only (I-LAN) or to allow access to the DHS Sensitive but Unclassified (SBU) network if authorized. The DHS Wi-Fi system shall be JITC certified. The DHS Wi-Fi system shall support seamless mobility and accurate location services for monitoring by DHS Operations personnel.

C.4.2.1.1.7.3.2 Wireless Intrusion Detection System (WIDS)

The TIP Contractor shall design a Campus-wide wireless intrusion detection system (WIDS), which at a minimum shall meet the following requirements:

- Continuously monitor Wi-Fi activity for wireless related intrusions on DHS wired and wireless networks Campus wide to include in-building protection
- Federal Information Processing Standards (FIPS) 140-2 certified
- Joint Interoperability Test Command (JITC) certified
- Certified under the National Information Assurance Partnership (NIAP) Common Criteria as meeting applicable U.S. Government protection profiles for basic or medium robustness environments, as determined and approved by the DHS Delegated Approving Authority (DAA)
- Continuously scan for and detect unauthorized activities. Continuous scanning is defined as 24 hours per day, 7 days per week, 365 days per year (24X7X365)
- Inclusion of a location-sensing protection scheme that detects wireless access attempts by identifying and locating unauthorized activity sources. The WIDS location-sensing capability must provide information that enables designated DHS personnel to take appropriate actions
- Utilization of a separate antenna system from IEEE 802.11 Wi-Fi design mentioned above
- Provide for the following defensive capabilities at a minimum: RF surveillance (IEEE 802.11, 2.4 GHz and 5 GHz frequency ranges), known vulnerability and attack detection (signature based), network anomaly-based threat detection, rogue wireless AP discovery, detection of authorized and unauthorized clients/devices, detection and assessment of DHS security policy deviations, physical location awareness of wireless devices, interference detection and spectrum analysis, mobile ad hoc network detection and packet and forensic analysis of wireless traffic
- Provide for GPS location transmission suppression

C.4.2.1.1.7.4 Satellite Communications

Due to historical property restrictions, there shall not be an extensive or significant satellite dish/antenna farms. The TIP Contractor's design shall support the following regarding satellite

communication:

- Support establishment of Campus Satellite Connectivity when required via DHS ONENET.
- Distributed the Campus Primary Satellite connectivity and redundancy to the Campus from any number of the four (4) Campus demarcs via wired connection.
- Support the establishment, connectivity, and service for the Campus single Mobile Satellite Connection Facility (pad), to be provisioned to support two to three mobile satellite trucks for connectivity to the infrastructure and electrical power. The Mobile Satellite Facility will be down-the-hill adjacent to the Warehouse/Large Vehicle Screening area, which will require a conduit run for fiber connectivity, power connections, and a concrete pad to accommodate the Mobile Satellite Trucks.
- Establishment and service the Campus two (2) smaller 8 foot Satellite Dishes to be installed in the ravine area above the Central Utility Plant (CUP) where they will be required to blend with existing structures and demography due to National Historic Preservation requirements.
- Support requirements that may include microwave, antennas, and iridium phones.
- Establish and support associated infrastructure such as radios, amplifiers, and fiber-optic connectivity

The satellite communication (SATCOM) terminals shall meet and adhere to the Programmatic Agreement and Section 106 of the National Historic Preservation Act (NHPA). The procurement of satellite time or transponders shall not be required.

C.4.2.1.1.7.5 Secure point-to-point high speed wireless services

The TIP Contractor shall design secure point-to-point high-speed wireless capability for DHS network redundancy and survivability. The campus network shall have the ability to establish point-to-point external connectivity to end points in the National Capital Region (NCR), which may be required to provide backup communications for DHS networks. The technologies may include, but are not limited to, free-space optics and millimeter wave technologies. The systems and/or equipment shall be JITC certified.

C.4.2.1.1.8 Internet Protocol Version 6 (IPv6)

DHS will require the TIP Contractor to research and recommend, where appropriate, the incorporation of IPv6 into the campus infrastructure. At a minimum however, core, distribution and access devices will adhere to the most recent version of the UCR IPv6 requirements.

C.4.2.1.1.9 Integrated Service Desk and IT Service Support Model

The TIP Contractor shall determine the service desk and IT service support model needed to service DHS employees operating within the Campus. The IT Service Support Model shall

include service levels for measurement, metrics for accountability, Tier 1 Service Desk support, Tier 2 Desktop Support, and Tier 3 Engineering Services. The IT service support model shall support and service all campus staff, technologies, and operations. The TIP Contractor shall design the DHS Service Desk to be Help Desk Institute (HDI) certified.

C.4.2.1.2 SYSTEMS

C.4.2.1.2.1 Voice Over Internet Protocol (VoIP)

The TIP Contractor shall be responsible for the design of a robust Campus-wide voice over internet protocol (VoIP) telecommunication system. The Campus VoIP system shall be based on the open and industry-standard Session Initiation Protocol (SIP) and Secure SIP. Although there may be a need to have unique "number" plans for both the USCG and other DHS Components due to inter-operations with groups not located on the Campus, this shall be accomplished using the virtual PBX capabilities of VoIP and systems such as but not limited to the open source telephony Asterisk. The TIP Contractor shall consider softphone applications,wherever possible, Power over Ethernet (PoE) shall be utilized on Campus.

C.4.2.1.2.2 Audio/Visual

The TIP Contractor shall design both classified and unclassified audio-visual video teleconferencing (AV/VTC) systems for the Campus. The TIP Contactor shall design and integrate the following technologies and systems:

- Video walls/displays
- Knowledge walls
- Conference room camera and display units
- Campus Media Center
- Press Center
- Hitchock Hall Auditorium and Conference Center
- Room management and reservation (Campus-wide)
- System servers and control units
- Video matrix recorders
- Video over IP
- Bridging Systems into campus signage

AV/VTC designs shall encompass Campus offices, conference rooms and centers, auditoriums, multi-media rooms, and the Campus Media Center. All AV/VTC systems shall comply with DHS standards. Identification and deployment of AV/VTC technologies will be tied closely with facility constructions. There will be approximately 500 conference rooms on campus that will be plumed for AV/VTC service.

C.4.2.1.2.3 Networks

The TIP Contractor shall design all elements of Campus network infrastructure considering the following objectives: high availability, security, flexibility, cost effectiveness, efficiency, robustness, and scalability. The TIP Contractor shall design the Campus networks to include:

- Sensitive but Unclassified (SBU)
- HSDN (Secret)
- HTSN (Top Secret -CLAN)
- SIPRNet (Secret)
- JWICS (TS-SCI)
- CGOne (SBU .MIL)
- Other specialized SCI networks

The TIP Contractor shall identify these services and develop the appropriate processes to provide seamless support while maintaining security requirements. The final Campus solution must interface with and support the above networks. The USCG facility will interface with both both "dot MIL .mil" and DHS "dot GOV .gov" domain on the Campus. But as a "dot MIL .mil" organization, the USCG systems and infrastructure shall need to meet all Department of Defense (DoD) security requirements, as well as DHS security requirements. The USCG-specific network requirements are for connectivity to the CGOne (SBU), SIPRNet (Secret), JWICS (Top Secret), and I-LAN (Internet only). The TIP Contractor shall identify and address these needs during requirements analysis.

C.4.2.1.2.3.1 Internet Only Access LAN (I-LAN)

The IT Contractor shall be required to design, install, operate, and maintain a logically segmented/separated Internet only (I-LAN) access capability via the Campus infrastructure that can be connected via a building network drop (Ethernet or optical) or RF Mobility Service Wi-Fi network access.

C.4.2.1.2.3.2 Networks

The TIP Contractor shall design infrastructure to support the following DHS networks. The TIP Contractor shall develop and present service levels and metrics to demonstrate performance expectations, uptime/availability, and ensure compliance with DHS management directives.

C.4.2.1.2.3.2.1 DHSNET (A LAN) – St. Elizabeths SBU Network

C.4.2.1.2.3.2.2 .MIL (NIPRNET)

C.4.2.1.2.3.2.3 Physical Security Networks

C.4.2.1.2.3.2.4Classified Networks

The TIP Contractor shall design infrastructure to support the following classified networks:

- HSDN (DHS SECRET Network)

- SIPRNET
- HTSN (DHS Top Secret Network) (C-LAN)
- JWICS

C.4.2.1.2.4 Cable Televison (CATV)

Approximately 400 sources of High Definition (HD) and internet protocol (IP) video shall be available on the Campus. DHS requires a cable TV system with a robust subscriber management system that is moveable and changeable, and able to operate with the anticipated Campus infrastructure. The TIP Contractor shall design a fiber-optic based subscriber based cable TV system (video over IP capable). Access via the subscriber management system (user privileges) shall be based on DHS Component security clearances and authorization. The system shall be used in conjunction with the Campus infrastructure operating on Campus. The purpose of this system is to distribute cable TV channels, locally created, commercial, and sourced operations (i.e., video and television) and to display archived recordings as well as training videos on an on-demand basis. These technologies must be capable of distribution down to the individual desktop computer.

C.4.2.1.2.5 Desktop Images

The TIP Contractor shall design a common desktop image for the Campus. DHS component offices may require additions specific to their mission.

C.4.2.1.3 SPECIAL FACILITIES

The TIP Contractor shall design all IT, physical security, IBS, and infrastructure supporting the following DHS special facilities. Details for the special facilities are included in Attachment E.

C.4.2.1.3.1 DHS Operation Center (DOC)

The TIP Contractor shall design systems and infrastructure supporting the DHS Operations Centers Facility (DOC), which shall house the Operations Coordination and Planning Directorate (OCPD), the National Operations Center (NOC), which operates as the DHS Secretary's hub for component operations centers during an event, the Enterprise Operations Center (EOC), other DHS co-located operations centers, and related support space. The DOC shall be approximately 366,800 gross square feet and shall be predominantly underground. The DOC shall support all levels of National Security Information (NSI) processing and display. The DOC will have approximately 850 daily staff occupancy with surge support for up to 3400 staff.

C.4.2.1.3.2 Enterprise Operations Center (EOC)

The TIP Contractor shall design systems and an infrastructure supporting an Enterprise Operation Center (EOC) (currently, the Headquarters Operations Center [HOC]) to monitor, manage, and perform problem resolution support of all Campus DHS Components, which consists of network circuits and devices, computer systems, applications, and databases/file servers. The purpose of the EOC is to monitor systems 24X7X365. The EOC will reside within

the DOC ITOC-1. The EOC will be located and maintained as a TS/SCI SCIF environment. The TIP Contractor shall use the EOC to monitor and manage all network enclaves using industry-standard applications. The TIP Contractor shall ensure that the EOC interfaces with the NOC located within the DOC and C-SOC (Physical Security Operations), including escalation procedures.

C.4.2.1.3.3 Campus Security Operations Center (C-SOC)

The TIP Contractor shall design systems and infrastructure to support the Campus Security Operations Center (C-SOC) to be located within the DOC. The C-SOC will provide a point of control, dispatch, and monitoring for all physical security and life safety on the Campus. These Security Operations shall be monitored 24X7X365 days per year and shall include, but shall not be limited to, access control and surveillance, including approximately five thousand cameras and card readers at various internal and external entry and exit points and surveillance platform locations. These servers and equipment will be supported via the physical security equipment room, which will be located within the DHS Operations Center. The TIP Contractor shall be required to design the physical security equipment room, install the appropriate racks and equipment, and provide operations and maintenance support.

There will be another C-SOC located on the campus, C-SOC 2. The C-SOC 2 will be located within the FEMA facility to be constructed in Post Phase 1. The C-SOC 2 shall be designed to completely take over the mission and operations of C-SOC 1 in case of emergency or shutdown of C-SOC 1.

C.4.2.1.3.4 Information Technology Operations Center (ITOC)

The TIP Contractor shall design systems and infrastructure supporting the Information Technology Operations Centers (ITOC-1 and ITOC-2), which will be the primary location for Tier 3 Engineer Services, EOC, Sensitive but Unclassified (SBU) and Classified Server Rooms, and Core Layer routing and switching for the Campus. All IT operational monitoring shall be accomplished within the ITOCs, as well as other Campus-wide and enterprise-wide systems, including voice telephony and network traffic destined for a location external to the Campus. There are two (2) ITOCs located on the Campus. ITOC-1 will be located within the DHS Operations Center and will serve as the primary location. ITOC-2 will be located within the USCG facility and will serve as the “dot MIL .mil” primary network infrastructure and serve as the continuity of operations (COOP) location for ITOC-1.

There shall be no server rooms in any Component space other than the DOC, USCG, and the ITOCs. The TIP Contractor shall not design, purchase, install, or maintain any server farms whatsoever on the Campus other than those approved for installation within the ITOCs. The TIP Contractor shall be required to design the Server Room, install the appropriate racks, and provide operations and maintenance (O&M) support for ITOC Server Rooms and for DHS servers approved for installation on the Campus. The gross square footage of Server Rooms is as follows:

- SBU Room: 2,100 gsf

- SCIF Room: 600 gsf
- USCG SBU Data Floor 5,000 gsf
- USCG Open Secret Data Floor 1550 gsf
- USCG Top Secret Data Floor 975 gsf

Space management is of paramount importance on the Campus. The TIP Contractor shall justify placement of any temporary or permanent servers on Campus on a case-by-case basis based on technical, performance, or redundancy requirements (e.g., packetization delays, propagation delays, or servers associated with video conferencing or security) with the Campus IT Program Manager and obtain specific written approval. The servers approved for immediate installation are print servers, domain controllers, desktop image storage servers, video recording and cache servers, and initially limited virtual desktop computers, etc. Additionally, the TIP Contractor is authorized to provide minimal servers as backups and redundancy on a temporary basis as part of the initial transition during all three Phases of Campus construction.

C.4.2.1.3.5 Computer Support Facilities (CSF)

The CSFs will be the primary location for information technology TIP Contractor staff provisioning, providing Tier 2 (T2) desktop support and some limited Tier 3 (T3) engineering support. It is anticipated that a total of seven to ten (7-10) CSFs will be distributed throughout the Campus. CSFs will be placed within major facilities and co-located with a cluster of facilities where the total numbers of staff do not warrant the construction of a dedicated CSF. There will be two (2) CSFs located within the USCG Headquarters (HQ) building. The USCG HQ CSF will directly support staff working within the building. The staff shall provide T2 desktop support, LAN support, and infrastructure support for "dot-MIL (.mil)" service. The T3 services in the initial USCG CSF shall be migrated into ITOC-1 once operational. During construction, the additional USCG HQ CSF shall be located within the DOC. The DOC CSF shall support all T2 Desktop support for those Components operating within the DOC. There will be two (2) CSFs located within the Center Building. The Center Building CSF will directly support executive level staff working within the building and will require a higher IT support staff to building staff ratio.

C.4.2.1.3.6 Sensitive Compartmented Information Facility (SCIFs)

The TIP Contractor shall design systems and infrastructure supporting the approximately 50 Sensitive Compartmented Information Facilities (SCIF) on the Campus. It is anticipated that 25 SCIFs will be located in the DOC. There will be compartments with nested levels of different classifications within the respective SCIFs. There may be SCIFs within SCIFs. There may be modular/moveable SCIFs. The Phase 1 Construction Contractor shall build-out and/or install the SCIFs. All SCIFs will be managed by DHS Office of the Chief Information Officer (OCIO), Office of the Chief Security Officer (OCSO), and Consolidated Headquarters Physical Security Division (CHPSD), in conjunction with respective DHS Component personnel. The TIP Contractor shall design the SCIF information technology infrastructure and operations. This may also include Uninterruptable Power Sources (UPS) when "red/black" power is required.

C.4.2.1.3.7 Test and Development Lab

The TIP Contractor shall be required to initially design a test laboratory to support the unclassified and classified test, development, and technology. The TIP Contractor shall provide its own existing test lab initially to support this effort. The initial test lab shall be located in the national capital region. A segment of the test lab shall be capable of handling tests of Top Secret information. The test lab shall support all proposed technologies that will be placed within production. The TIP Contractor shall design, establish, and present for approval the initial classified and unclassified test lab and subsequent on campus test labs. This effort should include the movement of the test lab from the initial location to the final campus locations.

C.4.2.1.3.7.1 Unclassified Network Lab

The unclassified lab is estimated to include a 1,635 USF large workroom and a 150 USF storage room. The workroom is anticipated to accommodate two (2) work benches with room for five (5) people, for a total of ten (10) people in the lab. There should be space for six (6) independently cooled racks that can be co-located within the lab. Secure storage space for equipment shall also be provided.

C.4.2.1.3.7.2 Classified Network Lab

The classified lab is estimated to include a 2,228 USF large workroom, a 180 USF storage room, a 144 USF Secure Equipment Room, and 180 USF office for a SSO. Electronics lockers will be required for equipment unapproved for lab access (i.e. cell phones, lap tops, etc). The workroom is anticipated to accommodate two (2) work benches with room for five (5) people, for a total of ten (10) people in the lab. There should be space for six (6) independently cooled racks that can be co-located within the lab. Secure storage space for equipment shall also be provided.

C.4.2.1.3.8 Multimedia Rooms

The TIP Contractor shall coordinate and design audio-visual (A/V) and infrastructure for the Campus Media Center, Press Center, Auditorium/Conference Center, and other media related requirements.

C.4.2.1.3.8.1 Campus Media Center

The Campus Media Center (CMC) will house the DHS Office of Public Affairs (OPA) personnel responsible for live imagery (television, video, etc.), still imagery (photographic), and graphic media production. In addition to the office space associated with these personnel, the CMC will house the following:

- Live Imagery Media – one (1) large and two (2) small traditional hard set television studios, with associated control rooms and storage that are also equipped to function as virtual studios. Other aspects of the CMC include editing suites, voice over booths, deployable equipment storage, electronics shop, construction shop, green rooms, and tape storage.

- Still Imagery Media – one (1) large photographic studio for group or large item photographs, one (1) small photographic studio for portraiture and sensitive items requiring a secure environment, an associated green room, and storage.
- Graphics Arts Media – The graphics personnel will predominantly work from their desk tops, but will be supported by a Media Print Production Lab. The Print Lab is expected to house the following types of equipment:

    - Wide width printer
    - Plotter
    - High quality, high capacity photo printer (all sizes)
    - Laminator
    - Multipurpose copier (collate, staple, etc)
    - Binding machine
    - Rimage
    - Shrink wrap machine
    - Cutting board and foam core board and mounting areas

Of the equipment listed, some is table top mounted while others will be free standing or require counter space to receive the documents as they are ready. Additional machines may be required to handle sensitive materials.

C.4.2.1.3.8.2 Press Center

The DHS Press Center will be operated by the DHS Office of Public Affairs, and will contain a 125 seat press briefing room, an attached interpreter booth, a control room, two (2) green rooms, journalist filing booths, a technical operations center, the DHS Secretary's Interview room (capable of tape/TV broadcast), and a media technical room. External media organizations will be able to tape/broadcast from inside the Press Briefing Room, at predetermined locations at the back of the room. All broadcast feed from the Press Center will route through the CMC. The Press Center will have connectivity to the remote satellite truck parking facility located near Gate 6.

C.4.2.1.3.8.3 Hitchcock Hall Auditorium and Conference Center

The DHS Auditorium, Hitchcock Hall, is a 700+ seat auditorium and conferencing center. The auditorium contains two (2) levels of seating, and should contain the following:

- Microphone/amplification of voice between audience and speaker for live interaction
- Internet connectivity at the seat level
- Video telecasting capability
- Presentation projection capability

The auditorium also acts as a backup Press Center when press briefing needs exceeds the Press Center capacity. Therefore, the auditorium requires designated locations for broadcast cameras with power supplies and connectivity to satellite parking, via the CMC.

The conference rooms located in Hitchcock Hall have no requirements above the standard requirements for all conference rooms on Campus.

C.4.2.1.3.8.4 Additional Media Related Requirements

Stand-Up Locations - external media will require "stand-up" locations at pre-designated locations around the Campus. These locations require power for television cameras, and associated equipment, and connectivity to the satellite truck parking lot, via the CMC. Locations will be determined by the DHS Office of Public Affairs.

Remote Media Satellite Truck Parking – a parking lot for external media satellite vehicles will be located along the Interstate Highway 295 access road, near Gate 6. The lot will support media outfits, with direct connectivity to the Press Center, via the CMC.

C.4.2.1.4 ASSET MANAGEMENT

The TIP Contractor shall design an asset management system. Assets are defined as all hardware and software assets, software licenses, wireless devices, copiers, printers, fax machines, telecommunication equipment, and any other DHS designated-accountable IT property. Any asset the TIP Contractor designs, procures and installs shall be tracked by the system. The asset management service must be able to provide real time assessment and understanding of the infrastructure in order to facilitate acquisition, receive assets, store, reconcile receipts with purchases, record descriptive elements and costs of its assets, distribute, locate, track, update, arrange for retrieval, store surplus, decommission, and remove assets from inventory.

C.4.2.2 SUBTASK 2 – PHYSICAL SECURITY

The TIP Contractor shall design an integrated physical security infrastructure for physical security systems listed considering the following security components:

- Ported coax sensor systems
- Fence sensor system
- Bi-static microwave systems
- Mono-static microwave systems
- Dedicated perimeter intrusion system (infrastructure equipment)
- Perimeter map display system
- Crash lighting system with local and central control system
- Hydraulic and electric bollards and plate barrier control systems
- Environmental day/night tube cameras
- Outdoor true day/night dome cameras
- Thermal image security cameras
- Analog and digital cameras
- Analog and digital video switchers
- Video Recording Archive System

- Video analytics
- Mega-pixel camera systems
- Video monitoring
- Network Video Recorder (NVR) system
- Under Vehicle Surveillance/Inspection Systems (UVSS) or (UVIS)
- Life safety duress systems (Campus-wide)
- Fiber and copper security infrastructure
- Security equipment racks and hardware
- Enterprise Access Control System - Campus wide (EACS)
- Intrusion Detection System (IDS) systems for SCIF and non-SCIF areas
- Classified Access Control System (CACS)
- Visitor management system
- HSPD-12 card readers systems
- Proximity card readers
- Card readers with PIN and/or Biometric (Multiplex System)
- Turnstiles
- Metal detectors (fixed and portable)
- Hand held metal detectors
- Package X-Ray – belt driven
- Pallet X-Ray
- Truck X-Ray
- Personnel CBRNE detection systems
- Vehicle CBRNE detection systems
- Isotope identification system (radiation detection system)
- Toxic chemical detection system

C.4.2.2.1 ACCESS CONTROL

The TIP Contractor shall design a robust suite of access control systems. The access control systems must integrate with the DHS HSPD-12 identification cards. The access control will include the systems and equipment listed below and any equipment/systems identified in this task:

- Security head end equipment
- Magnetometers
- Physical security systems
- Security force
- Vehicle access parking garage gates
- X-ray machines

The access control experience, system design, infrastructure, and support shall include, but not be limited to the following:

- Design and install an Access Control Systems (ACS) within an integrated large site or Campus system that meet Interagency Security Committee (ISC) Level 5 standards
- Design and install a multi-agency Visitor Management Systems to include the visitor facility that meets ISC Level 5 standards
- Design and install access control systems for high security areas such as ISC Level 5 Government Operations Center and Special Compartmental Information Facilities (SCIF) with operations at the Top Secret/SCI security level
- Design and install an Intelligence Community Badging System (ICBS). TIP Contractor employees shall have approved or certified Governmental clearance levels to conduct ICBS installations
- Design and install a dedicated Electronic Security Systems and Access Control Systems within the LAN/WAN infrastructure
- The TIP Contractor shall be capable of performing Pre-Installation and Testing Check Out (PITCO) testing for every system, subsystem, and component of the prior-to-final installation
- This TIP Contractor shall be an issuing authority for UL-2050 certificates that meet all DCID 6/9 SCIF requirements. ICD 705 regulations have replaced the DCID 6/9 standards and the TIP Contractor must be prepared to adhere to this new requirement

C.4.2.2.2 LIFE SAFETY

C.4.2.2.2.1 Multi-Media Emergency Notification Systems/Public Notification Systems (ENS/PNS)

The TIP Contractor shall design multi-media notification and life safety systems that will be expandable and maintainable for the future. The system must provide audio, visual, and data based notification to all Campus residents. The system shall, at a minimum, include capabilities to distribute and communicate via a public address (PA) system, email and text notification, Campus television/monitors (IPTV/kiosks/digital signage), and Campus-dispersed emergency call stations. This approach shall require outside coordination at all levels (i.e., local state and federal Government and law enforcement agencies). The system shall integrate with the fire alarm enunciation system.

C.4.2.2.2.2 External Life Safe Communications

The Campus must communicate with the District of Columbia (DC) first responders and on-site personnel. The Campus-Security Operations Center (C-SOC) will get real-time feeds from the DC Command Center, and they in-turn will receive feeds from the Campus. Fire support shall alert multiple locations such as the C-SOC, GSA, DHS, guard shacks, and the DC Command Center. The on-Campus Public Safety Answering Point (PSAP) will be in the C-SOC and serve as the primary location.

C.4.2.2.2.3 Emergency Call Stations

The TIP Contractor shall be responsible for designing an interactive emergency call and information station, Emergency Call Station (ECS), with multiple points on the Campus. The purpose of the ECS is to provide effective and immediate "Open-Line" crisis communication and response to those in need. When an emergency is taking place, it is vital that security personnel can quickly identify the location and nature of distress and respond accordingly. The ECS shall integrate video surveillance (CCTV), cellular phone technology, and two-way radio and access control systems. The ECS units shall have such features as, strobes, video camera, internet protocol (IP) for power over Ethernet, hands-free one button operation, microphone, speaker, and other safety features to further enhance the security web. The ECS shall be suited to fit many different installation methods such as self-standing, pole, and wall. The ECS shall be equipped with the appropriate look and necessary options for its determined location.

The ECS shall be installed in parking garages, along outdoor walkways on Campus, or indoors. All ECS locations must acquire government approval regarding the most optimal location for placement. Units shall meet Americans with Disabilities Act (ADA) and Section 508 requirements including location message.

C.4.2.2.3 PERIMETER SECURITY

C.4.2.2.3.1 Video Surveillance

There may be up to 5,000 security cameras on the Campus. These cameras will be at gates, doors, entry points, and perimeter fencing as approved by DHS Security. There will be lighting/motion detectors with Infrared Light Emitting Diodes (IFR LED). The TIP Contractor shall interface with DHS to design and determine where to place the cameras and motion detectors and to determine site lighting types and levels. Video recording and playback shall be required.

C.4.2.2.4 SECURITY OPERATIONS MANAGEMENT

C.4.2.2.4.1 Guard Force Communications

The TIP Contractor shall design the infrastructure and equipment associated with the two-way radio system for use by the guards and other Government and contractor personnel. The TIP Contractor shall include service levels and metrics concerning availability, service, and inventory.There will be a temporary guard force and facility during construction and permanent guard force post occupancy.

C.4.2.2.4.2 Security Operations

The TIP Contractor shall design elements of the security enterprise operated by DHS Security. Physical security monitoring will take place in the C-SOC by DHS personnel. DHS Security will maintain control over the entire Campus.

C.4.2.3 SUBTASK 3 – INTELLIGENT BUILDING SYSTEMS (IBS)

GSA Public Buildings Service (PBS) has selected the St. Elizabeths Campus as a pilot project to implement its new Smart Buildings Program (SBP). The SBP focuses on:

- Buildings—progressive and experimental use of systems and methods)
- Technology—captures and analyzes data for continuous optimization and results measurement
- People—transform staff with skill sets for next generation building information management

Buildings on Campus shall be monitored and controlled by a Campus-wide enterprise smart buildings application. The TIP Contractor shall design and provide the control and monitoring application and hardware and the transport system. These systems must interface with the off-Campus and on-Campus Governmental operation centers and acquire DHS Certification and Accreditation. The TIP Contractor shall be responsible for the design and installation of the applications and associated hardware for the following systems:

- Building Automation Systems (BAS) – HVAC controls, Energy Management
- Power Monitoring Equipment and Subsystems
- Critical Facility/Data Center Systems
- Access Control and Security Systems
- Lighting Controls
- Intelligent Fire Protection
- Parking Guidance Systems
- Digital and Interactive Signage (Content Management with digital media players)
- Shuttle Tracking System
- Conference Room Reservation System

The TIP Contractor's IBS shall comply with the four (4) principles:

- Open Protocol
- Native Power
- Convergence
- Normalized

The TIP Contractor's design for IBS shall consider relevant GSA PBS data architecture as a model.

C.4.2.3.1 OPEN PROTOCOLS

The TIP Contractor shall provide open protocols for all controls systems and IT. No proprietary protocols will be considered acceptable. Open protocols include the Internet Protocol (IP) wherever possible. Where controls or technologies do not support or operate using IP, then the

industry-standard for open protocol for each trade will be required. For example, electrical and some other metering should use Modbus and Modbus IP. The Lighting controls system shall communicate at the panel level with Building Automated Controls Network (BACnet). Proprietary protocols will not be allowed in the management server, floor level controllers, or the edge devices. The HVAC controls systems shall be either LonWorks or native BACnet. Native BACnet is an ANSI/American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) standard and is supported by National Institute of Standards and Technology (NIST) and the Lawrence Berkley National Laboratories, and shall mean the following: each edge or field device for BACnet controls should contain the BACnet protocol stack and be interchangeable or "plug and play" with any controller. Further, the device field level protocol shall be the standard protocol for communications between HVAC devices such as VAV terminal units, fan coil units and rooftop units. All field level devices shall communicate on the local operating control network via one of the following protocols and product requirements: LonTalk EIA-709.1 utilize free topology transceiver (78K baud rate) implemented on all HVAC control devices and requiring LonMark Certification or BACnet ANSI/ASHRAE Standard 135-2004 in which the field bus shall be BACnet MS/TP at minimum of 38.4 baud and the HVAC control devices shall conform to BACnet device definitions for BAAC or B-ASC and require BACnet Testing Laboratory (BTL) certification.

C.4.2.3.2 NATIVE POWER

The TIP Contractor shall be responsible for designing an infrastructure that provides edge devices direct current power notably in the form of power over Ethernet (PoE) when applicable. Examples include security cameras, access controllers, clocks, telephones, lighting controllers, and digital media players. The infrastructure will leverage PoE devices that can power many and sundry devices such as phones, clocks, video surveillance cameras, access control, and other devices. The TIP Contractor shall be responsible for advising if their controls and edge devices can be specified to use PoE. The security network infrastructure is exempt from the PoE requirement.

C.4.2.3.3 CONVERGENCE

C.4.2.3.3.1 Controls Connectivity

The TIP Contractor shall comply with all codes and regulations and design a current day, robust, secure controls backbone that will be utilized by all building systems and experience systems. The backbone will consist of fiber, cabling, enclosures, electronic switching, routing and fiber optic termination gear, uniform power supplies, data back-up equipment, and other components. The TIP Contractor shall be the backbone provider for all inter-connections required for all building controls systems in the project except for fire life safety and possibly conveyance, depending on the vendor and design. This means that the design and specification shall make it clear that after horizontal (usually serial) cabling terminates in a floor-level controller, the TIP Contractor shall not provide further cabling or network infrastructure for their system, and will be provided with a port(s) to connect to that will link to their other floor-level controllers and the systems management server. The TIP Contractor shall locate their controllers in designated

locations such as a mechanical, electrical, or telecom rooms where the backbone ports will be available.

C.4.2.3.3.2 Controls Servers

The management servers for every control system shall be provided by the TIP Contractor and shall reside in a designated location in the building. Each controls supplier shall submit to the TIP Contractor the server capacity and performance requirements. Those servers shall maintain the proper specifications and requirements such as virus protection, firewall, power, UPS, redundancy, and data back-up. The location of the controls systems will be in the ITOCs or other designated locations. Additionally, the controls system management servers shall be purchased, managed, and serviced by the TIP Contractor.

C.4.2.3.4 NORMALIZED

The TIP Contractor shall design each core system, which while functioning independently, shall also be connected to a middleware appliance to normalize the data generated from disparate devices and systems in order to provide the opportunity for interoperability and consumption of building systems data by back office software systems. This includes interoperability between building systems, IT systems, and security systems to provide seamless information sharing, notification, and management.

C.4.2.3.5 CENTRAL UTILITY PLANT (CUP)

The Campus Central Utility Plant (CUP) provides backup power through gas turbine and backup diesel generators. The CUP is the command and control center for the distribution of chilled water, heat, and electricity. The current contract for operating the CUP is with Washington Gas. The TIP Contractor shall be responsible for connecting into the CUP systems controller provided by the Construction Contractor. This shall be an optical or Ethernet connection that will be routed back to a set of CUP application servers provided by the TIP Contractor in the GSA designated field office(s). The CUP server will be connected to an operations console provided by the TIP Contractor to monitor data from the CUP and other buildings on Campus.

C.4.2.3.6 ADVANCED PARKING MANAGEMENT SYSTEM

The TIP Contractor shall design an Advanced Parking Management System (APMS). The APMS shall provide both directional information and space availability information.

The APMS is a Campus-specific system that shall provide parking information utilizing variable messages signs, i.e., passive and active components, which provide real-time information about the availability of parking at the appropriate decision points. The system shall be designed to provide information such as which lots are full and how many spaces are available, as well as have signs on every floor of each garage, at the start of every aisle, and in front of every individual parking space.

In its planning and designing of the APMS, the TIP Contractor shall be responsible for determining what type of system will count the vehicles in the facility (entry/exit counters and space occupancy detectors) and also the type of communication system, i.e., how will the components of the system will communicate with each other – digital fiber optic communications versus RF transmitters. The TIP Contractor shall also consider the dynamic parking environment, whether parking configuration will change requirements over time, periodic repaving, etc.

At a minimum, the APMS shall be comprised of active and passive signs, remote sensors, central computer, communications infrastructure, and power infrastructure. Another component of the APMS is the acquisition, location, and operations of the vehicle variable electrical charging stations. The TIP Contractor shall be required to design a variable vehicle charging system located within the parking garages. Consideration shall be given to future changes to the system that could incorporate other garages off Campus.

C.4.2.4 SUBTASK 4 – ENTERPRISE MANAGEMENT SYSTEMS (EMS)

The TIP Contractor shall design an overarching ITIL aligned EMS. The system shall integrate the management of **all systems and infrastructure installed by the TIP Contractor** to include IT, physical security, and IBS. The system shall allow operators at all the DHS Operation Centers on the Campus to monitor and manage their respective functional area. Servers for the system shall reside in the ITOC-1 and ITOC-2. This system at a minimum shall provide the ability to manage the following: network operations (manager of managers), trouble ticket requests, change and configuration management, work flow operations management and asset management. The TIP Contractor shall propose the Enterprise Management System in their proposal and discuss the rationale for selection. This system shall be capable of seamlessly integrating with other DHS and DHS Component service desk applications (multiple) to transfer tickets. There will be separate EMS per classification of data, however COI separated networks are expected to share EMS with appropriate C&A and security partitioning in place.

C.4.3 TASK 3: IMPLEMENT, TEST, AND SECURE SOLUTION (OPTIONAL)

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit, and transition to operations and maintenance (O&M) of all IT, physical security and Intelligent Building Systems designed and approved in the Requirement Analysis and Design Task.

Testing - The TIP Contractor shall test all technologies for functionality, operability, and interoperability prior to delivery. Testing shall include demonstrating capabilities via presentation of a proof of concept. DHS will review all test and proof of concept presentations to verify that the technologies being presented perform within specific specifications and parameters. DHS personnel will be responsible for formal acceptance after successful completion of all tests. The TIP Contractor shall initially establish a test network in the TIP Contractor provided test lab per C.4.2.1.3.7. Upon completion of facilities, establish an on-Campus test network. The TIP Contractor shall be required to equipment, design, setup, update, and maintain both the initial off-campus and Campus test network. Prior to any implementation

of technologies, all changes or modifications to existing or proposed technologies shall be required to use the DHS change management processes and procedures.

Security and Accreditation - Specifically, the TIP Contractor shall support the security processes, controls, and tools that provide information assurance among the enterprise networked services, in accordance with DHS Management Directives (MD), the National Institute of Standards and Technology (NIST) Special Publications (SP 800 series), Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Director of Central Intelligence Directives (DCID) and the Intelligence Community Directives (ICD). The TIP Contractor shall directly support the DHS Risk Management Division (RMD) in their oversight of security compliance of all systems relative to DHS security policies, guidance, and mandates.

C.4.3.1 SUBTASK 1 - INFORMATION TECHNOLOGY

C.4.3.1.1 INFRASTRUCTURE

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit, and transition to operations and maintenance the following infrastructure as designed and approved in the Requirement Analysis and Design Task of DHS TIP:

C.4.3.1.1.1 Campus and Building Wiring

C.4.3.1.1.2 Passive Optical Network – Access Layer

C.4.3.1.1.3 Zones – Distribution Layer

C.4.3.1.1.4 Campus fabric

C.4.3.1.1.5 Core Layer

C.4.3.1.1.6 Off-Campus Connectivity

C.4.3.1.1.6.1 Demarc Points

C.4.3.1.1.6.2 ONENET Access and Integration

C.4.3.1.1.6.3 Remote Satellite Connectivity

C.4.3.1.1.6.4 Defense Information Systems Network (DISN)

C.4.3.1.1.7 Radio Frequency Mobility Service

C.4.3.1.1.7.1 Mobile Wireless Communications, to include mobile phones for the Campus DHS users

C.4.3.1.1.7.2 Land Mobile Radio (LMR) to include two-way Radios for the DHS LMR users.

C.4.3.1.1.7.3 Wireless Networking Capability

C.4.3.1.1.7.3.1 Wi-Fi

C.4.3.1.1.7.3.2 Wireless Intrusion Detection System (WIDS)

C.4.3.1.1.7.4 Satellite Communications

C.4.3.1.1.7.5 Secure Point-to-Point High Speed Wireless Services

C.4.3.1.1.8 Internet Protocol Version 6 (IPv6)

C.4.3.1.1.9 Integrated Service Desk and IT Service Support Model

C.4.3.1.2 SYSTEMS

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit, and transition to operations and maintenance the following systems as designed and approved in the Requirement Analysis and Design Task of DHS TIP:

C.4.3.1.2.1 Voice Over Internet Protocol (VOIP) System to Include End Item VOIP Phones.

C.4.3.1.2.2 Audio/Visual

C.4.3.1.2.3 Networks

C.4.3.1.2.4 Cable Television (CATV)

C.4.3.1.2.5 Desktop Image (St. Elizabeths Core and component specific additions)

C.4.3.1.3 SPECIAL FACILITIES

The TIP Contractor shall purchase, implement, perform proof of concept, and operational testing, configure, accredit, and transition to operations and maintenance all IT, physical security, IBS, and infrastructure as designed and approved in the Requirement Analysis and Design Task for the following DHS special facilities:

C.4.3.1.3.1 DHS Operation Center (DOC)

C.4.3.1.3.2 Enterprise Operations Center (EOC)

C.4.3.1.3.3 Campus Security Operations Centers (C-SOC)

C.4.3.1.3.4 Information Technology Operations Centers (ITOC)

C.4.3.1.3.5 Computer Support Facilities

C.4.3.1.3.6 Sensitive Compartmented Information Facility (SCIFs)

C.4.3.1.3.7 Test and Development Lab

C.4.3.1.3.8 Multimedia Rooms

C.4.3.1.3.8.1 Campus Media Center

C.4.3.1.3.8.2 Press Center

C.4.3.1.3.8.3 Hitchcock Hall Auditorium and Conference Center

C.4.3.1.3.8.4 Additional Media Related Requirements

C.4.3.1.4 ASSET MANAGEMENT

The TIP Contractor shall purchase, implement, perform proof of concept, and operational testing, configure, accredit, and transition to operations and maintenance the Asset Management System as designed and approved in the Requirement Analysis and Design Task.

C.4.3.2 SUBTASK 2 - PHYSICAL SECURITY

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit and transition to operations and maintenance the following physical security systems as designed and approved in the Requirement Analysis and Design Task of DHS TIP:

C.4.3.2.1 Access Control

- TIP Contractor shall demonstrate the capability and resources to design a multifaceted system with migration and cutover of no–downtime ACS/IDS
- The TIP Contractor shall be capable of performing Pre-Installation and Testing Check Out (PITCO) testing for every system, subsystem, and component prior to final installation.
- This TIP Contractor shall be an issuing authority for UL-2050 certificates that meet all DCID 6/9 SCIF requirements. ICD705 regulations have replaced the DCID 6/9 standards, and the TIP Contractor must be prepared to adhere to this new requirement.

C.4.3.2.2 Life Safety

C.4.3.2.2.1 Multi-Media Emergency Notification Systems/Public Notification Systems (ENS/PNS)

C.4.3.2.2.2 External Life Safe Communications

C.4.3.2.2.3 Emergency Call Stations

C.4.3.2.3 Perimeter Security

C.4.3.2.3.1 Video Surveillance

C.4.3.2.4 Security Operations Management

C.4.3.2.4.1 Guard Force Communications

C.4.3.2.4.2 Security Operations

C.4.3.3 SUBTASK 3 - INTELLIGENT BUILDING SYSTEMS (IBS)

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit and transition to operations and maintenance the following Intelligent Building Systems as designed and approved in the Requirement Analysis and Design Task of DHS TIP:

- Building Automation Systems (BAS) – HVAC controls, Energy Management
- Power Monitoring Equipment and Subsystems
- Critical Facility/Data Center Systems
- Access Control and Security Systems
- Lighting Controls
- Intelligent Fire Protection
- Parking Guidance Systems
- Digital and Interactive Signage (Content Management with digital media players)
- Shuttle Tracking System
- Conference Room Reservation System
- Central Utility Plant (CUP)
- Advanced Parking Management System

C.4.3.4 SUBTASK 4 – ENTERPRISE MANAGEMENT SYSTEMS

The TIP Contractor shall purchase, implement, perform proof of concept and operational testing, configure, secure, accredit and transition to an overarching ITIL aligned EMS.

C.4.4 TASK 4 - Operations and Maintenance (OPTIONAL)

The TIP Contractor shall provide operations and maintenance (O&M) services for the IT implementation at the Campus. This includes but is not limited to O&M of IT, physical security, Intelligent Building Systems, and equipment implemented under the DHS TIP effort, to include the underlying IT Campus infrastructure and transport. Other O&M services required are

configuration and change management, IT asset migration support to include life cycle replacement and technical refresh, continuity of business, continuity of operations, warranty support for installed equipment and material, network and security management across all classifications of networks, and the operation of a Tier 1 Service Desk with an associated enterprise application suite to promote Information Technology Infrastructure Library (ITIL), Projects in Controlled Environments (PRINCE 2), and Control Objectives for Information and Related Technology (COBIT) aligned enterprise service and project management processes, as well as providing Tier 2 Desktop/End Item and Tier 3 Engineering support.

The TIP Contractor shall use ITIL and Change Management for the creation of a configuration management system with clear and defined procedures that captures technology insertion to capitalize on standards declaration. The change management program shall incorporate a basic repository of IT infrastructure components and their relationships, but quickly expands into a bold vision for IT knowledge management. Emphasis should be placed on transitioning IT from a systems management perspective (e.g. server xyz is down) to a "service" management perspective (e.g., the order entry system is down).

The TIP Contractor shall provide a comprehensive O&M Plan for the DHS TIP addressing all the requirements and deliverables set forth in this Section. All SOPs, SLAs, Plans, and Checklists identified in this Section shall be included as sub-deliverables under the comprehensive O&M Plan.

C.4.4.1 SUBTASK 1 - ENTERPRISE SERVICES

C.4.4.1.1 APPLICATION SERVICES

C.4.4.1.1.1 Service Desk ITIL Based Enterprise Management Suite

The TIP Contractor shall provide and operate a Tier 1 ITIL based Service Desk Enterprise Management Suite to support the Campus user community. There are currently multiple enterprise management suites utilized by various DHS Components. Coordination and communication (transfer of service request tickets) with various DHS Component Help Desk software shall be available for implementation.

C.4.4.1.1.2 Enterprise Application Connectivity

Enterprise applications are outside the scope of DHS TIP except those required to support on-Campus systems (e.g., fire, parking, notification, security, and building management systems). DHS primary applications such as SharePoint and Exchange email are located in the data centers, as are most Component-specific applications. These will continue to be supported by the existing support contractors.

The TIP Contractor-specific enterprise applications such as the Service Desk Enterprise Management Suite may be housed on-campus or placed within the DHS data center.

DHS requires that the IT network and desktop platform be seamless, giving personnel the ability to access authorized networks and authorized applications independent of physical location on the campus. The TIP Contractor shall provide a template of services that each Component can pick from to meet their specific application needs. Component-specific applications will ride on top of this and be supported by existing processes.

The TIP Contractor shall be responsible for supporting, facilitating, and ensuring access to Enterprise applications from the Campus location. Once data leaves the Campus the responsibility shifts to the designated DHS responsible party. Applications the TIP Contractor shall coordinate connectivity include but are not limited to:

- Exchange
- Remedy Service Desk
- SharePoint
- Oracle
- Juniper
- Imanami Web Directory
- DHS Virtual Private Network
- MS Project Server
- MS Communicator

C.4.4.1.2 CLOUD CONNECTIVITY

C.4.4.1.2.1 Demarcation Points

The TIP Contractor shall operate and maintain equipment implemented under Section C.4.3 within the demarcation facilities.

C.4.4.1.2.2 ONENET

The TIP Contractor shall coordinate with the ONENET Program Management Office (PMO) for any operational requirements relating to ONENET. The TIP Contractor shall follow the DHS Authority to Operate (ATO) procedures, Certification & Accreditation (C&A), conduct proper security test and evaluation (ST&E), and use the DHS configuration management processes while interfacing with ONENET.

The TIP Contractor shall not be responsible to support ONENET installed and operated equipment.

C.4.4.1.2.3 I-LAN

The TIP Contractor shall operate and maintain a logically segmented/separated Internet only network that shall be connected via building network drop or Wi-Fi network access. Network drops located within classified locations shall not have this access.

C.4.4.1.3 SERVER ROOMS

The TIP Contractor shall be required to provide O&M support for equipment installed within the ITOC server rooms, the physical security equipment room, and for DHS servers approved for installation on the Campus.

C.4.4.2 SUBTASK 2 - FACILITIES

C.4.4.2.1 INTELLIGENT BUILDING SYSTEMS (IBS)

The TIP Contractor shall maintain all IBS systems and infrastructure installed under DHS TIP. All buildings on-Campus shall be monitored and controlled by a Campus-wide enterprise smart buildings application. The TIP Contractor shall operate and maintain the control and monitoring applications, servers, hardware, and interface with off-Campus and on-Campus operation centers.

The systems include, but are not limited to:

- Building Automation Systems (BAS) – HVAC controls, energy management
- Power monitoring equipment and subsystems
- Critical facility/data center systems
- Multimedia/audiovisual systems
- Access Control and Security Systems
- Lighting controls
- Intelligent fire protection
- IT Infrastructure
- Parking guidance systems
- Digital and interactive signage (web-based content management with digital media players, room reservation system)
- Shuttle tracking system
- Conference room reservation system
- CUP systems controller
- Vehicle charging system

C.4.4.3 SUBTASK 3 - INFRASTRUCTURE

C.4.4.3.1 CAMPUS AREA NETWORK (CAN)

C.4.4.3.1.1 Campus Fabric

The TIP Contractor shall operate and maintain all Campus fabric systems and infrastructure installed under DHS TIP. The TIP Contractor shall operate and maintain the following:

- Indoor distributed antenna systems wireless (DAS)
- Intrusion detection and prevention (IDPS)
- Network Security

- Distribute antenna system (hand held and cellular)
- Outdoor distributed antenna system wireless
- DHSNet SBU network connectivity
- Virtual private network (VPN) access
- Virtual desktop service (rack mounted desktops)
- Wireless clock, transmitters and antennas
- Wireless security
- AV/VTC connectivity
- Passive Optical Network (PON)

C.4.4.3.1.2 Audio Visual (A/V)

The TIP Contractor shall operate and maintain A/V systems and infrastructure installed under DHS TIP. The TIP Contractor shall operate and maintain the following:

- Video walls/displays
- Knowledge walls
- Conference room camera and display units
- TV and photographics studios
- Press Center
- Room management and reservation (Campus wide)
- System servers and control units
- Video matrix recorders
- Video over IP

AV/VTC support shall be provided by the TIP Contractor to Campus offices, conference rooms and centers, auditoriums, multi-media rooms, and the Campus Media Center.

C.4.4.3.1.3 Operations Management

C.4.4.3.1.3.1 DHS Operation Centers Facility (DOC)

The TIP Contractor shall operate and maintain systems and infrastructure supporting the DHS Operations Centers Facility (DOC), which will house the Operations Coordination and Planning Directorate (OPS), the National Operations Center (NOC), the Enterprise Operations Center (EOC), and other DHS co-located operations centers, and related support space. The DOC will support all levels of National Security Information (NSI) processing and display.

C.4.4.3.1.3.2 Information Technology Operations Centers (ITOCs)

The TIP Contractor shall operate the ITOCs, which are the core operations centers for managing network related operations, providing help desk Tier 3 (T3) engineers, and engineering support for projects. The TIP Contractor shall monitor network availability (all networks and classifications), respond to network emergencies, provide Tier 3 Engineer services, and support the ICCB Change Management process. The ITOCs are the central locations for on-Campus

network demarc (this is where the core of the network will route on Campus and off-Campus traffic).

C.4.4.3.1.3.3 Enterprise Operations Center (EOC)

The TIP Contractor shall operate the EOC and monitor, manage, and perform problem resolution support of DHS Components, which consist of network circuits and devices, computer systems, applications, and databases/file servers. The purpose of the EOC is to monitor systems 24X7X365. The EOC will be located and maintained in a TS/SCI SCIF environment. The TIP Contractor shall use the EOC to monitor and manage all network enclaves using industry standard applications and shall segregate, both logically and physically, maintain, and operate EOC systems by security classification level. The TIP Contractor shall ensure that the EOC interface with the DHS Operations Center (NOC) and the C-SOC 1 located within the DOC, including escalation procedures.

The TIP Contractor shall provide the following service:

- Monitor network devices, environmental systems (HVAC, UPS), or peripheral devices which are managed or monitored to quickly detect, track, isolate, and resolve problems.
- Perform troubleshooting techniques to isolate the source of, diagnose and/or resolve, or assist in the resolution of network problems (end-to-end) and root cause analysis.
- Develop and submit the EOC Standard Operating Procedures (SOP) to the TPOC or designated representative for review and approval.
- Operate the EOC and support DHS COOP exercises. The TIP Contractor shall perform tests as requested by designated DHS personnel quarterly, at a minimum, and as required by the co-develop COOP Policy (developed post award) to verify failover from primary to backup EOC (ITOC) without any disruption of operational capability.
- Support Continuity of Government (COG) exercises. The TIP Contractor shall perform tests as requested by designated DHS personnel per the co-developed COOP/COG standard operating procedures (SOP). The TIP Contractor shall facilitate and participate in the development of the COOP/COG SOPs.
- Identify the requirements for and install upgrades, updates, service packs, and patches.
- Maintain security protection and reliability updates on operating systems.
- Identify and notify designated DHS personnel of any upgrades, updates, service packs, and patches determined to be incompatible with system or application specifications and proceed as directed.
- Monitor system operability and functionality, identify abnormal performance and degradation, and complete resolution actions and return the system to normal performance.
- Monitor system capacity, maintain normal performance, and prevent system degradation resulting from usage exceeding system capacity.
- Operate the EOC to respond to changes in loads on the network as necessary in response to higher threat levels.
- Report on the network and systems infrastructure using an Enterprise Management Tool. The TIP Contractor shall report on network and system status as directed by

designated DHS representative to include Network Diagrams that identify enterprise building, floor, room, rack, and system for HQ and field sites.

- Notify and update the Help Desk, CSF, and DOC of any network or system infrastructure issue or problem detected or managed by the EOC.
- Manage status, errors, and inbound and outbound traffic statistics of all routing interfaces, bandwidth utilization, and errors of all inbound and outbound LAN/WAN/VLAN circuits.
- Provide after-action reports for outages that are significant (priority 1 or 2) within 48 hours of the system or network that has been restored and work with the resiliency team in ensuring future outages are mitigated through recommendations.
- Manage the LAN/WAN routing protocol between the routers and OLT's. Perform port management, network capacity management (including planning and trending), and configuration management.
- Maintain configuration LAN/WAN change documentation, and continually update schematics to reflect current network architectures in accordance with the DHS ICCB.
- Support terminal equipment associated with special circuits as required and maintain and monitor connections to designated off-Campus locations.
- Maintain and monitor the secure wide area network connection to existing and/or future connections to other Intelligence Community's networks.
- Provide Network Metrics Reports to the DHS-designated representative.
- Maintain the outbound and inbound Internet access to ensure full operational capability for internal and external user contiguous hours access to the Internet 24X7X365 except during periods of Government approved planned outage. The TIP Contractor shall provide outbound access connectivity for the DHS staff to the Internet. The TIP Contractor shall provide in-bound public access connectivity to the DHS Public Website.
- Coordinate with authorized vendors in monitoring Internet access, identify, and resolve interruptions to the Internet service. The TIP Contractor shall perform upgrades, implement changes, and install patches to Components on the Internet servers. These shall include middleware updates, new Database Source Networks (DSNs), application updates, application additions, patches, and hot fixes.
- Perform all maintenance that will disrupt or could disrupt the availability of Internet services only during planned outage periods.
- Maintain logs of Internet activity and make available for review as requested by DHS designated representatives.
- Adhere to the DHS perspective in Enterprise Interconnection and Policy Working Group (EIWG) with DoD to facilitate the technical issues and governance processes related to the interconnection between the Secure Internet Protocol Router Network (SIPRNET) and DHS secure networks, address operational problems, and assist in extending capabilities to Federal information sharing initiatives.
- Attend meetings of and contribute to specific technical operational working groups set up to address engineering and operations issues with DoD and other Governmental agencies, and leverage the TIP Contractor knowledge and resources to ensure that DHS is aligned with emerging Intelligence Community (IC) systems engineering and technology solutions.

C.4.4.3.1.3.4 Campus Security Operations Centers (C-SOCs)

The TIP Contractor shall provide IT technical operations and maintenance support to IT equipment supporting the Campus Security Operations Center 1 (C-SOC 1) and Physical Security Equipment room to be located within the DOC. The TIP Contractor shall also provide IT technical operations and maintenance support to IT equipment supporting the C-SOC 2, in FEMA Headquarters (failover/backup). The TIP Contractor shall provide a point of control, dispatch, and monitoring for all physical security and life safety on the Campus. The TIP Contractor shall provide 24X7X365 technical support that includes, but is not limited to, the operations and maintenance of access control and surveillance, including approximately 5,000 cameras and card readers at various internal and external entry and exit points, and surveillance platform locations, and servers supporting this activities.

C.4.4.3.1.4 Passive Optical Network (PON)

The TIP Contractor shall operate and maintain PON components and infrastructure installed under DHS TIP. This shall include but is not limited to the following:

- Inside building cable plant fiber-single mode
- Dual Filament Fiber
- Campus PON equipment OLT-SBU
- Campus PON equipment MUTOA-SBU
- Campus PON equipment ONT-SBU
- Campus PON equipment OLT-Classified
- Campus PON equipment ONT-Classified
- Inside building cable plant copper
- Copper (Special Program circuits)
- Inside Cable Plant Termination cost - fiber
- Outside Campus PON Cable Plant
- Patch panels and racks (fiber and copper)
- Copper - ONT to desktop
- SCIF fiber distribution

C.4.4.3.2 CONNECTIVITY

C.4.4.3.2.1 Networks

The TIP Contractor shall operate and maintain networks and infrastructure installed under DHS TIP.

The TIP Contractor must interface with existing systems such as HSDN (Secret), HTSN (Top Secret CLAN), DoD SIPR/NIPR/JWICS, .MIL, and specialized SCI services. The TIP Contractor shall identify these services and develop the appropriate processes to provide seamless support while maintaining security requirements. The TIP Contractor shall provide

these services for each network:

- Server Room Services
- Desktop Support Services
- End User Equipment
- IT Security
- O&M Engineering Services
- Physical Security Equipment Room Services
- Project Engineering Services
- Switch and Routers Services
- Encryption Device Services

C.4.4.3.2.2 CATV

The TIP Contractor shall operate and maintain the Campus CATV system and infrastructure installed under DHS TIP. The TIP Contractor, in conjunction with DHS, shall operate a fiber-optic based subscriber based cable TV system. Access via the subscriber management system (user privileges) shall be based on DHS security clearances and authorization.

C.4.4.3.2.3 Point-to-Point Wireless

The TIP Contractor shall operate and maintain point-to-point wireless systems installed under DHS TIP, to include millimeter wave and free space optic solutions.

C.4.4.3.2.4 Satellite

The TIP Contractor shall operate and maintain satellite systems and infrastructure installed under DHS TIP.

C.4.4.3.2.5 Telephone/Fax

The TIP Contractor shall operate and maintain telephones and fax analog connectivity and infrastructure installed under DHS TIP.

C.4.4.3.2.6 VOIP

The TIP Contractor shall operate and maintain the VOIP System and infrastructure installed under DHS TIP. This shall include at a minimum the following:

- COOP VOIP equipment and service
- VOIP backbone
- VOIP network equipment (servers)
- Phones to include wall and conference room phones

C.4.4.3.2.7 Equipment

The TIP Contractor shall operate and maintain the following equipment installed under DHS TIP. This shall include the following:

- Core border routers ITOC-1 and ITOC-2
- Personal secure residential phones
- Termination equipment
- Uninterruptable Power System (UPS)
- Server room racks (water cooled with UPS)

C.4.4.3.3 MOBILITY SERVICES

C.4.4.3.3.1 Wireless Network Access (Wi-Fi)

The TIP Contractor shall operate and maintain the Wi-Fi system and infrastructure installed under DHS TIP.

C.4.4.3.4 SUPPORT SERVICES

The TIP Contractor shall operate and maintain support equipment installed under DHS TIP.

Support equipment such as printers, copiers, scanners, plotters, and fax machines shall be dispersed throughout the Campus. The TIP Contractor shall be required to purchase, install, operate, maintain, repair, and support service equipment for the Campus. This includes the purchase, storage, and distribution of printer accessories such as toners cartridges, inks cartridges, and plotter pens.

C.4.4.3.5 WIRELESS SERVICES (CELLUAR, UHF, AND VHF)

The TIP Contractor shall operate and maintain all wireless systems and infrastructure installed under DHS TIP.

The Contactor shall support the acquisition, distribution, accountability, and disposition of designated Government issued cellular, UHF, VHF, two-way phones and hand held devices for staff assigned to work on the Campus. This service includes:

- Coordinating with appropriate wireless carriers for service support and coverage
- Coordinating with appropriate carriers for pager service
- Coordinating and facility the acquisition and the inclusion of SME-PED devices

C.4.4.4 SUBTASK 4 - PHYSICAL SECURITY

The TIP Contractor shall operate and maintain physical security systems and infrastructure installed under DHS TIP to include, but not limited to the following security components:

- Ported coax sensor systems

- Fence sensor system
- Bi-static microwave systems
- Mono-static microwave systems
- Dedicated perimeter intrusion system (infrastructure equipment)
- Perimeter map display system
- Guard crash alarm system
- Crash lighting system with local and central control system
- Hydraulic and electric bollards and plate barrier control systems
- Environmental day/night tube cameras
- Outdoor true day/night dome cameras
- Thermal image security cameras
- Analog and digital cameras
- Analog and digital video switchers
- Video Recording Archive System
- Video analytics
- Mega-pixel camera systems
- Video monitoring
- NVR system
- Under Vehicle Surveillance/Inspection Systems (UVSS) or (UVIS)
- Life safety duress systems (Campus-wide)
- Fiber and copper security infrastructure
- Security equipment racks and hardware
- Enterprise access control system (Campus-wide)
- IDS systems for SCIF and non-SCIF areas
- Classified access control system
- Visitor management system
- HSPD-12 card readers systems
- Proximity card readers
- Card readers with PIN and/or Biometric (Multiplex System)
- Turnstiles
- Metal detectors (fixed and portable)
- Hand held metal detectors
- Package X-Ray – belt driven
- Pallet X-Ray
- Truck X-Ray
- Personnel CBRNE detection systems
- Vehicle CBRNE detection systems
- Isotope identification system (radiation detection system)
- Toxic chemical detection system

C.4.4.4.1 ACCESS CONTROL

The TIP Contractor shall operate and maintain the access control system and infrastructure installed under DHS TIP.

- Personnel
  - Security force facilities
  - Visitor Control Facility
  - X-ray machines
  - HSPD-12 Cards
- Physical
  - Access control equipment
  - Security head end equipment
  - Magnetometers
  - Physical security systems
- Vehicular
  - Vehicle access parking garage gates

C.4.4.4.2 LIFE SAFETY

C.4.4.4.2.1 Multi-Media Emergency Notification Systems/Public Notification Systems (ENS/PNS)

The TIP Contractor shall operate and maintain the Multi-Media ENS/PNS systems and infrastructure installed under DHS TIP.

C.4.4.4.2.2 External Life Safety Communications

The TIP Contractor shall operate and maintain the external life safety communications and infrastructure installed under DHS TIP.

C.4.4.4.2.3 Emergency Call Stations

The TIP Contractor shall operate and maintain the Emergency Call Stations and infrastructure installed under DHS TIP.

C.4.4.4.3 SECURITY OPERATIONS MANAGEMENT

C.4.4.4.3.1 Guard Force Communications

The TIP Contractor shall operate and maintain the infrastructure and equipment associated with the two-way radio system for use by the guards and other Government and Contractor personnel. There is a temporary guard force during construction and permanent guard force post occupancy.

C.4.4.4.3.2 Physical Security Operations

The TIP Contractor shall maintain the elements of the security enterprise operated by DHS Security. Physical security monitoring shall take place in the C-SOC by DHS personnel. DHS Security will maintain control over the entire Campus.

C.4.4.4.4 PERIMETER SECURITY

The TIP Contractor shall operate and maintain the Perimeter System and infrastructure installed under DHS TIP.

- In-building
  - Video surveillance cameras
- Perimeter and campus
  - Perimeter fence sensors
  - Crash intercom system
  - TW notification
  - Chem/bio/rad/nuc explosive detector systems
  - Video camera system
  - Video switching systems
  - Video recording systems

C.4.4.5 SUBTASK 5- SERVICE OPERATIONS MANAGEMENT

C.4.4.5.1 ASSET MANAGEMENT

The TIP Contractor shall operate and maintain the Asset Management System and infrastructure installed by the TIP Contractor under DHS TIP. All assets purchased under DHS TIP and assets brought onto Campus during the transition are covered under this Asset Management System.

C.4.4.5.2 SERVICE OPERATIONS

Hours of operation: the normal hours of operation are 6:00 A.M. to 7:00 P.M. Various functions require 24X7X365 coverage. The TIP Contractor should make recommendations for modifying and improving operating hours.

Operating Hours

Service Area	Work Hours
Core Service Hours	6 A.M to 7 P.M.
Network Management Operations	24X7X365
Security Management Operations	5x12 desktop support operations
COMSEC Operations	
Continuity Operations	
Operations and Maintenance for End User Support: • T1 Service/Help Desk • T2 Desktop Support • T3 Engineer Support	VIPs - on call support

Hours of operation other than normal: There will be mission situations that require the TIP Contractor to work other than normal hours. Such scheduling may require accomplishment of TIP Contractor work at times other than normal operation hours. Extreme weather conditions and natural disasters (such as tornados, flooding, snow, and ice) may warrant temporary office evacuation or office closure. The TIP Contractor shall respond to extreme weather conditions and shall inform all employees of these instructions. Facility closings shall in no way interfere with the TIP Contractor operation and maintenance of the critical systems. All TIP Contractor employees identified by the TIP Contractor as essential personnel shall remain on duty or report for duty in accordance with the Emergency Situations and relevant Continuity of Operations (COOP), IT Contingency, IT Disaster Recovery/Business Continuity Plans.

The TIP Contractor shall participate in all scheduled and unscheduled fire drills, Shelter in Place, and other scheduled safety and emergency-training exercises, which may necessitate interrupted services unless directed otherwise.

Building Occupant Emergency Plan Compliance: TIP Contractor personnel shall comply with all building occupant emergency plan activities such as building evacuations and shelter in place.

Personnel Response to IT Continuity Events: TIP Contractor personnel with critical skills shall report to and perform duties at alternate sites during IT continuity events, as directed by the Government. The TIP Contractor shall provide personnel resources to respond to IT continuity events. The TIP Contractor should consider such things as cross-training and providing personnel who would be able to respond from outside the metropolitan area (i.e. individual with appropriate skill sets who would be unaffected by issues in the Baltimore-Washington, DC metropolitan area).

Performance of Services During Crisis: The following services are essential during crises declared by the DHS Secretary or the President of the United States. All basic services and operations shall continue. The TIP Contractor shall submit an essential personnel list, to include designated emergency POCs, to the COR. The list shall contain the individual's name, address, home phone number, cell phone number, security clearance, and duty title. Upon notification of a crisis, the TIP Contractor shall implement the developed disaster recovery COOP plans. All plans shall incorporate DHS standards and procedures in their development. All plans are subject to DHS approval.

The TIP Contractor shall provide within the CONOPS a detailed end-user and Desk Side Support Concept of Operations that includes elements such as a detailed description of processes, procedures, policies, WBS, organization chart, work flow, detailed performance metrics, and evaluation criteria for the entire help desk/service desk operations, including Tiers 1, 2 and 3. The end-user and Desk Side Support Concept of the Operations Plan shall demonstrate a proactive and aggressive methodology to pursue new IT technological advancements and trends applicable to help desk/service desk and desk side support such as conducting frequent and thorough market research and analysis of new IT technologies and equipment including software based upon a subjective and comparative analysis to existing DHS technology.

The TIP Contractor's Concept of Operations Plan shall meet the following minimum requirements:

- Provide continuous operation 24X7X365 helpdesk and desk side support operations, with the provision that designated VIPs are entitled to on call support, which includes call center support, Network Systems Monitoring, Tier 1 (help desk/service desk services) including remote desktop management for Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) applications and Tier 2 (Desk Side Support) services as well as Tier 3 (Engineering Support) for diagnosing and resolving end user problems unresolved by the second-level analysts.
- Help desk/service desk operations through Tier 3 Engineering Support: The TIP Contractor shall design the help desk/service desk to act as the primary interface to the end users of various COTS and custom-developed applications. Users shall have the option to address their help desk/service desk requests through a toll free telephone number and/or through the DHS Intranet. DHS currently has email and telephonic help desk/service desk contact capabilities, and the TIP Contractor shall propose additional contact methods (web, chat) to increase the accessibility of the help desk/service desk. The TIP Contractor shall provide seamless call distribution and call management support.
- The TIP Contractor shall design, implement, and maintain a DHS-approved COTS enterprise help desk/service desk system capable of interfacing and reporting to DHS systems as required.
- This system shall provide a knowledge base for technicians and provide self-help for end-users. All data generated, stored, and maintained in the system remains the property of the Government.
- The TIP Contractor shall provide on-site and field office support comprised of personnel with appropriate level of security clearances who shall resolve complex technical problems of laptops, desktops, network peripheral devices, network components, storage devices, and troubleshooting of various software- and hardware-related issues.
- The TIP Contractor shall provide infrastructure advanced operational support and infrastructure services to DHS. The TIP Contractor shall perform troubleshooting to isolate the source of, diagnose and/or resolve, or assist in the resolution of IT and telecommunications problems (end-to-end).

C.4.4.5.2.1 Service Desk - Tier 1

The TIP Contractor shall be required to establish an off-Campus, CONUS, Tier 1 (T1) IT service desk of the Campus to receive requests for IT service. The service desk shall serve as the initial point of entry for requests (IT, facilities, and security). The service desk shall be a TIP Contractor-owned-Contractor operated (COCO) facility. The TIP Contractor shall ensure that the DHS Service Desk is Help Desk Institute (HDI) certified within the first three (3) months of the service desk activation.

C.4.4.5.2.2 Desktop Support Tier2

The TIP Contractor shall provide level Tier 2 Desktop Services and respond to and resolve Tier 2 service desk requests that cannot be processed by the Tier 1 IT service desk. The Tier 2 staff shall be distributed throughout the Campus for mandatory support and co-location. All Tier 2 desktop service staff shall be located within DHS Facilities and shall have primary responsibility

for servicing the DHS staff located within their assigned buildings. As the Campus construction is completed and DHS staff moves into their respective Campus facilities, the level of Tier 2 support is expected to increase incrementally.

C.4.4.5.2.3 Engineering Services Tier 3

The TIP Contractor shall provide Tier 3 Engineering Services in support of help desk/service desk requirements, Campus network related activities, and project management activities. For help desk/service desk support the TIP Contractor shall respond to Campus only requests for service that cannot be resolved by Tier 2 service desk technicians. This position is final escalation and should be designed to support call ticket/service desk request for service. Campus network related service shall include but not be limited to server specific request, network outages, and limited subject matter expertise. Engineer services in support of project management shall provide access to staff to support efforts towards the design, configuration, setup, implementation, test and evaluation, and limited subject matter expertise for all IT projects. This may, on occasion, require the coordination with outside vendors, non-St. Elizabeths DHS Components, and designated staff and organizations.

C.4.4.5.2.3.1 Certification and Accreditation (C&A)

The Certification and Accreditation (C&A) phases as outlined in NIST 800-37 revision 1 are inherently Governmental tasks. The TIP Contractor shall supply appropriate staff to support all other phases of this process to include but not limited to the Initiation and Monitoring phases of the Certification and Accreditation Process, including but not limited to, ISSO duties as documented in NIST 800-37 revision 1. This applies to any and all FISMA systems hosted at this facility. The TIP Contractor shall supply resources qualified to perform ISSO duties for all current and future FISMA systems hosted at this facility. Formal C&A submissions shall be a joint responsibility of the TIP Contractor and Government system owner. All C&A activities must comply with designated DHS and/or DOD guidelines and policies to include Government acceptance of TIP Contractor resources. All systems shall include non-traditional IT, such as building automation, TV studio, Audio-Visual, and physical security, and will require C&A to operate.

C.4.4.5.2.3.2 Desktop Software Images

DHS operates in a diverse architecture environment. The TIP Contractor shall be required to coordinate with each DHS Component, determine current image requirements, establish the technical infrastructure to support multiple images, and establish processes and procedures to support each Component’s specific desktop software image packages.

To prepare for a future common operating environment, DHS is currently working on a consolidated plan for common software imaging for workstations. The plan includes applications, operations systems, and any and all other security authentication requirements that may be necessary for universal usage. It is anticipated that DHS will adapt a universal software image. The TIP Contractor shall coordinate with the current DHS-wide common imaging

software plan to bridge the current requirements with future desktop software image requirements.

C.4.4.5.2.3.3 Data Migration and Backup

For Campus moves and changes, the TIP Contractor shall include the migration of data, if required, from the original system to the new system. The TIP Contractor shall ensure the smooth and complete migration of data. This may include temporary storage of data when transitioning from the original system to a new system.

The TIP Contractor shall coordinate, facilitate, and support the development of a data backup strategy and standard operating procedures for all DHS Campus Components. The strategy shall include coordinating with data center staff to ensure backup services are available. The TIP Contractor shall establish a limited data backup infrastructure, backup services and support, and data recovery for the Campus. The backup and recovery service shall incorporate recovery time objectives, storage media, and escrow standards consistent with Government and commercial best practices. All data migration, backup, and recovery procedures, plans, and services shall be included in all disaster recovery plans.

C.4.4.5.2.4 Test and Development Lab

The TIP Contractor shall be required to operate and maintain the test laboratory implemented under DHS TIP to support the DHS IT Infrastructure Systems. The test lab, at a minimum, shall provide the following services and support:

- Support to developers and customers performing integration and test activities. The TIP Contractor shall provide support during the hours of 8:00 am ET to 5:00 pm ET, Monday – Friday, excluding Federal holidays. The TIP Contractor shall also provide support after hours, on weekends, and on Federal holidays for purposes such as deployments, maintenance, and extended testing support.
- Configuration changes in the test laboratory and production environments. The TIP Contractor shall plan for future configuration changes and production deployments in coordination with the DHS designated representative. The TIP Contractor shall make configuration changes in compliance with security policies and procedures and change control procedures. Configuration changes shall be in accordance with controlled and repeatable procedures established by the TIP Contractor.
- Documentation of test procedures and configurations performed by the TIP Contractor relating to the support of testing activities.
- Tracking of the status of actions and tasks performed by them in support of testing activities.
- Provide notification regarding any issues or risks that affect the performance of current or scheduled test activities. The TIP Contractor shall notify the TPOC within three (3) business days of discovery of an identified issue or risk that could affect performance of the test activities. The TIP Contractor shall provide a complete description of the issue, diagnosis, resolution actions undertaken, and the impact on the timeframe for test activities.
- Support authorized DHS requests for testing applications; installing software; verifying currency of installed software; and configuring security settings, databases, and user accounts and permissions.

- Create, update, and maintain standard workstation images, commonly referred to as ghosts, to support deployment to the desktop. The images shall meet all stated standards for "as-is" current production environment and "to-be" production environment. The TIP Contractor shall provide the integration and testing with the standard mechanism for delivery of the application to the desktop.
- Maintenance of web-based applications in the test environment by performing activities such as installing upgrades, patches and service packs, assigning user names and passwords, and assigning user permissions.
- Support to the Testing Lab by performing activities such as reviewing new application architecture, verifying that the application architecture supports the current DHS environment, and submitting findings to the TPOC.
- Perform a production readiness review in order to determine whether a system is ready for deployment into the production environment.
- Follow all designated DHS processes and procedures for configuration control, change management, risk management, and user testing and acceptance.

C.4.4.5.2.5 Project Management

All IT, construction, implementation, and deployment shall be classified as projects and shall be required to follow the DHS Program Governance Process as defined in Attachment F. All IT project activities will become part of the St. Elizabeths Portfolio of Projects. Staff designated to represent project related activities shall be designated as project managers or leads.

The TIP Contractor shall designate project managers for specific Campus projects. These project managers shall represent the TIP Contractor on all project related matters. The project managers shall follow DHS Governance, PMBOK, ITIL v2 and 3, PRINCE 2, and VaL IT best practices, implement and enforce compliance with the Project Management Lifecycle, and follow these general project management activities:

- Ensure the Project Team completes the project
- Develop the project plans and manage team performance of project tasks
- Secure acceptance and approval of deliverables from the Project Sponsor and stakeholders
- Ensure the project is delivered within budget, on schedule, and within scope
- Report on project status, risk management and escalation issues per the processes
- Acquire all required gate review approvals and ensure projects are managed through the PMLC
- Ensure contract deliverables are submitted in accordance with the contract
- Create and track Work Breakdown Structures (WBS)
- Create and lead project Integrated Project Teams (IPT)
- Keep Customer Relationship Managers (CRMs) informed regarding project status and potential problems
- Coordinate with required Government officials for aspects of managing projects to include moves/add or changes to activity, plans, and sites
- Conduct comprehensive assessment of project risk(s)
- Establish formal Risk Management Plan
- Present project risks as required to senior management
- Ensure risk mitigation deadlines are calculated as efficiently as possible, established, and adhered to
- Develop and report progress for risk management tasks

C.4.4.5.2.6 Training

The TIP Contractor shall provide professional, technical, and end-user training. The TIP Contractor shall provide the training support for DHS IT operations to include user applications and network access, system administration, and security. The TIP Contractor shall develop training plans for DHS personnel, system users, and contractor personnel. The training plans shall be submitted to the TPOC for approval prior to implementation. The TIP Contractor shall maintain an electronic record of all training courses conducted and who attended.

End-User Training

The TIP Contractor shall develop, document, and conduct end-user training on all COTS, GOTS, and unique software. The TPOC will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed sessions or via computer-based self-paced training. The TIP Contractor may elect to provide this training in incremental elements depending upon component usage, and may be delivered via computer-based training, help files, or instructed sessions following Government approval.

Security Training

The TIP Contractor shall develop, document, and administer a Security Training Plan and curriculum providing annual required security awareness and operational security refresher training. Delivered training elements shall comply with DHS and other relevant external agency directives and policies for enforcement of Government security provisions. The appropriate TPOC will review and approve the training curriculum prior to implementation. Implementation of the training may be either through instructed sessions or via computer-based self-paced training. The TIP Contractor may elect to provide this training in incremental elements depending upon component usage, and the training may be delivered via computer-based training, help files, or instructed sessions. The TIP Contractor shall provide training to users and operators to facilitate the usage of security components within the network and on the desktop.

System Administrator Training

The TIP Contractor shall provide appropriate training, training materials, and help desk/service desk support for the applications provided for DHS St. Elizabeths staff. The TIP Contractor shall work with the Government to develop a training plan that addresses the delivery of training to supervisors, and system administrators (includes TIP Contractor personnel and Government personnel). The plan shall be in conformance with the SOPs and SLAs. The TIP Contractor shall:

- Provide the training curriculum and training materials for DHS applications and desktops. The training materials shall be suitable for both users and system administrators, and adopted from existing training materials for legacy applications integrated into DHS service.
- Provide the delivery of the user training through a “train-the-trainer” approach to the maximum extent possible. The TIP Contractor shall provide training directly to the users on Campus.

- Provide DHS training through training delivery methods such as the following:
    - Direct delivery of the training to user and system administrators at DHS facilities.
    - Direct delivery of special user training to personnel who will then act as trainers.
    - Delivery of training to user through computer-based training (CBT) or other distance learning techniques that the TIP Contractor has found effective.
- Provide documentation and manuals for COTS products that have them.

C.4.4.5.2.7 IT Security Compliance

The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide a high-level of security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As such, all production systems on the DHS network at this location require security compliance and information assurance to a variety of federal mandates and DHS-specific policies as well as guidance. Specifically, the TIP Contractor shall support the security processes, controls, and tools that provide information assurance among the enterprise networked services, in accordance with DHS Management Directives (MD), the National Institute of Standards and Technology (NIST) Special Publications (SP 800 series), Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Director of Central Intelligence Directives (DCID) and the Intelligence Community Directives (ICD). The TIP Contractor shall directly support the DHS Risk Management Division (RMD) in the oversight of security compliance of all systems relative to DHS security policies, guidance, and mandates.

The TIP Contractor shall provide support of functions necessary to provide necessary security services to the DHS security compliance program, to include:

- Certification and accreditation-related (C&A) tasks including:
    - Provide support of relevant documentation including Standard Operating Processes and Procedures
- Information Systems Security Officer (ISSO) tasks including:
    - Maintain situational awareness through continual monitoring of all production systems at this location
    - Identify and report relevant security and operational weaknesses of all production systems at this location to the appropriate Information Systems Security Manager (ISSM) or assigned ISSO
    - Provide on-site security support in coordination with the operational security teams
    - Support vulnerability management efforts by the operational security teams
    - Report all security events and notification to the enterprise DHS SOC and relevant parties for escalation
- Ensure that all proposed changes of production systems go through the enterprise change management program. If necessary, perform validation and remediation of proposed changes to maintain or enhance existing security controls, processes, or procedures.

C.4.4.5.2.7.1 Security Systems Administration

The TIP Contractor shall manage and monitor all DHS security components, including intrusion detection systems (IDSs) and Policy Enforcement Points (PEPs). Security systems shall use an automated delivery function to the maximum extent possible to push anti-virus software signature updates to the desktops and provide the results to Information Technology Services Office STE EOC/SMC management for analysis. Security systems administration shall include the following:

- Monitoring of DHS systems for intrusion activity, and preparing to take appropriate steps to mitigate any suspected intrusion while maintaining the availability of the system for all authorized users.
- Conducting computer forensics, law enforcement evidence collection, and preservation efforts in support of the system.
- Conducting assessments quarterly (or as directed) at all major nodes, such as gateways and regional centers where data is stored and report the results of such findings to the DHS designated representative.
- Performing anti-virus scans of the entire DHS networks in accordance with the proscribed procedures in DHS Approved Maintenance Downtime.

C.4.4.5.2.7.2 Security Change Management

The TIP Contractor shall centrally manage and control the implementation of corrective patches and service packs, and required upgrades. All changes will be captured within either the DHS change management database (CMDB) or an authorized contractor developed CMDB. Changes may include but not be limited to:

- For all new installations, system upgrades or routine maintenance, the TIP Contractor shall complete all requested administrative requirements and testing prior to submission to DHS Governance approval.
- Assessment of DHS directed security patches or service packs before implementation to verify the need to implement and the impact upon the system.
- In coordination with DHS, determination of the schedule for deploying Information Assurance and Vulnerability Alerts (IAVAs), patches, and service packs.
- Providing monthly reports to the appropriate DHS designated representative on the success of the patch/service pack deployment, and any issues preventing completion.

C.4.4.5.2.7.3 Security Log Access, Retention and Review

The TIP Contractor shall maintain all security logs for the required retention period. Access to these logs shall be restricted to ISSM approved personnel, including:

- Recording all accesses to these logs, including an audit history of reads, changes, and deletions.
- Protecting logs under these restrictions to include all security logs (PEP, IDS, anti-virus), as well as domain controller and all management systems as directed by the ISSM/ISSO.
- Performing reviews and providing monthly reports (or as directed) on all system logs.

C.4.4.5.2.7.4 System Security Administrators

The TIP Contractor shall provide all System Security Administrators (SSA). Each SSA is an extension of the SMC in providing security oversight, monitoring, and reporting for DHS and is the principal POC for all security issues and support of Government ISSMs and ISSOs.

C.4.4.5.2.7.5 Data Spills and Response

The TIP Contractor shall employ guards and gateways to monitor, prevent, detect, respond, report, and correct the unauthorized release of classified data.

C.4.4.5.2.7.6 Incident Response

The TIP Contractor shall create and maintain the capability to respond rapidly to any network event that could affect the Information Assurance/Information Protection posture of DHS. The TIP Contractor shall create and maintain SOPs and checklists to cover events such as network intrusions, data spills, introduction of malicious software, Denial of Service (DoS) incidents, inappropriate network use, etc. The TIP Contractor shall base these SOPs and checklists upon existing DHS directives and guidance.

- The TIP Contractor shall maintain a trained Computer Security Incident Response Team (CSIRT), which may include systems administrators and other personnel. The TIP Contractor shall develop policies and processes related to the establishment and generation of the CSIRT. The CSIRT shall maintain a digital forensics capability that establishes and maintains an evidentiary chain of custody.
- The TIP Contractor shall utilize all available audit logs to support forensics activities, and shall develop SOPs for the conduct of forensics investigations that shall be submitted to the DHS designated representative for approval. The TIP Contractor shall follow established reporting procedures when providing initial notification to the SSAs, Security Manager, ISSO, and Information System Security Manager (ISSM) of any network event or incident.
- The TIP Contractor shall provide Event and Incident Reports to the Government as directed in the DOD-Dir.8500 Series Computer Network Defense (CND). The Continuity of Operations Plan shall detail non-IT incident response, as identified in HSPD-5 and the DHS Initial National Response Plan.

C.4.4.5.2.7.7 Information Condition (INFOCON) Management

In response to potential threats to DHS and U.S. infrastructure assets in general, the Secretary of the DHS may direct the elevation of the protection levels of the network and IT assets through the implementation of INFOCON levels. The INFOCON level is determined based upon an assessment of risk to the DHS networks. When directed by DHS, the Designated Accrediting Authority (DAA) will approve specific measures of protection for the networks. The TIP Contractor shall:

- Implement INFOCON conditions within the DHS, and shall track the attainment of the directed INFOCON level across the networks.
- Assist in the coordination of DHS INFOCON levels and that of external entities such as DoD as directed by the TPOC.
- Develop and follow SOPs and checklists to track the changes in INFOCON level and the attainment of the directed INFOCON.
- The Information Technology Services Office SMC shall create SOPs based upon DHS policies to support the DHS Computer Network Defense Continuity of Operations Plan.

C.4.4.5.2.7.8 Communications Security (COMSEC) Management

The TIP Contractor shall:

- Provide on-site 24X7X365 COMSEC support for services such as installation maintenance and administration of messaging systems (e.g., DMS, AMHS, receipt, transmission and/or distribution of all forms of communication media such as: faxes, messages, correspondence, etc).
- Operate encryption systems to support secure voice and video systems as required and assist Government personnel with receipt, inventory control, deployment, and securing of encryption systems. The TIP Contractor shall assist users in the operations of secure facsimile systems, and perform user level maintenance.
- Receive, distribute, inventory, and administrator COMSEC account material.
- Perform COMSEC technical tasks such as maintaining and updating messaging systems, installation, and maintenance of all cryptographic equipment (e.g., TACLANE, FASTLANE, and KIV-7).
- Provide a COMSEC Plan to address implementation and operational details in accordance with DHS and NSA policies and procedures and provide to the DHS designated representative.
- Establish and manage a COMSEC account in accordance with DHS guidelines and procedures.
- Manage, update, and maintain the Information Technology Services Office SMC COMSEC account and COMSEC controlled items (CCI) and all keying material.

C.4.4.5.2.8 Maintenance and Outages

The TIP Contractor shall perform maintenance and other related activities that degrade or may degrade the performance of network environments, operating systems, databases, and applications during outage periods that occur on weekends, Federal holidays, or between the hours of 10:00 pm ET and 6:00 am ET on weekdays. The TIP Contractor shall avoid performing these maintenance and other activities during periods of the year that require continuous availability 24 hours each day. When developing the maintenance and outage plan, the IT contractor must incorporate a minimum of one (1) week notice for scheduling after hours maintenance and outage. The TPOC or designated representative will notify the contractor a minimum of five (5) business days prior to periods requiring continuous availability.

C.4.4.5.2.9 Tech Refresh and Evolution

Currently, each DHS Component/Subcomponent is responsible for its own architecture and technology deployment. It is the DHS objective and goal to have a standard, uniform architecture and technology for the Campus. Operationally, this means that each DHS Component and Subcomponent will have the same consistent set of tools and technologies Campus-wide as designed and installed by the TIP Contractor available to them. Each DHS Component/Subcomponent may use only a subset of all the features that will be supplied as necessary to execute their mission.

C.4.4.5.2.10 Executive Telecommunications Support

The TIP Contractor shall provide contiguous hours (24X7X365) of secure and non-secure IT and communications services and support for the Secretary of DHS, the Deputy Secretary, and other designated DHS executive staff while they are traveling outside of the National Capital Region (NCR).

- The TIP Contractor shall provide daily operations support for fixed and mobile IT/telecom equipment such as the following tasks:
    - Manage and control inventory
    - Operate, test, troubleshoot, and maintain equipment
    - Operate and ensure capability of mobile IT/telecom vehicle
    - Maintain proficiency on existing and future IT/telecom systems
    - Assist in design, development, analysis, integration, and evaluation of IT/telecom systems
    - Plan and perform preventive maintenance inspections on IT/telecom equipment
    - Perform equipment lifecycle management
    - Perform COMSEC and project management support

- Synthesize customer needs with commercially available IT products into requirements that shall allow the implementation of engineered IT/telecom systems and processes
- Provide operational assistance to DHS Senior Executives and staff

- The TIP Contractor shall provide travel operations support such as:
  - Coordinate with DHS staff advance arrival personnel at the travel sites
  - Transport IT/telecom equipment to and from travel sites
  - Conduct site survey(s) for installation of travel systems
  - Install and remove IT/telecom equipment from trip site
  - Provide point-to-point telecom support to travel teams
  - Coordinate their own travel logistics arrangements

C.4.4.5.2.11 User Profiles

Seven (7) end user profiles were created for DHS TIP. The profiles of the end users are based upon their use of the network and requirements for service. End-user profiles are determined by the network type and required access to resources, amount and type of devices in use at their workstation, level of service and support needed to complete their work, and level of importance concerning their position and responsibilities. The profiles are as follows:

No.	End User	Profile	% of All End Users
1	Transient Workstation Users	Ad-hoc inquiry, web browsing, general information look-up. Usually from a shared workstations	1
2	Standard Users	Network access, enterprise resources, printers, special applications	73
3	Special Application Users	Use of specialized applications typically in operations centers	5
4	Administrative Users	Email accounts, web browsing, Microsoft© Office Product delivery, service desk, application support	6
5	Analysts and Investigative Users	Law Enforcement	9
6	Power Users	IT network administrators and Computer Professionals	5
7	Executive Users	Senior Executive Service	1
		Total	**100**

C.4.4.5.2.12 AD HOC REQUIREMENTS

The TIP Contractor shall provide management and technical information to the Government such as:

- Technical evaluation of suggestions
- Input for staff studies
- Fact sheets
- Audits
- Congressional inquiries
- One-time reports
- Material, equipment, facilities, and other property listings or inventories
- Equipment maintenance records
- Information requested by the COR and/or TPOC from the designated representative on other interfacing contracts that support this effort

C.4.4.5.2.13 Transition Services to Fixed Price Incentive Fee (FPIF)

After one (1) year of operations, the Government may transition to a FPIF basis for Operations and Maintenance (O&M) Support. The TIP Contractor shall perform all due diligence to identify the sum total of support tasks and present a revised cost proposal using fixed unit pricing for services.

C.4.4.5.3 SPECIAL PROGRAMS

The TIP Contractor shall provide O&M on IT equipment supporting DHS Special Programs Multimedia Rooms that include:

- Campus Media Center
- DHS Press Center
- Campus Auditorium
- Additional media related requirements

The IT support includes:

- Television studios
- Sounds rooms
- Broadcast rooms
- 700+ seat auditorium AV/VTC
- Interview rooms
- Media print production lab

C.4.5 Task 5 – PROVIDE technical consulting support (OPTIONAL)

The scope of DHS TIP includes IT, physical security, and IBS integrated in a Campus environment. During performance, the TIP Contractor shall retain the services of specific third - party vendors supporting applications and products deployed in the DHS architecture. The TIP Contractor shall provide technical consulting (e.g., engineering/consulting support for requirement definition, integration, testing, design reviews, application development, and security planning, wireless / Wi-Fi advances) directly to the Customer Relationship Management Division (CRMD), Customer Projects Office (CPO), St. Elizabeths Special Program Office. Technical consulting support services are limited to products, applications, and technologies already deployed in the DHS architecture. The TIP Contractor shall extend this technical consulting support directly to the DHS Component/Subcomponent upon direction from the TPOC or COR. The level of effort supporting this task is estimated to not exceed ten (10) FTEs annually.

C.4.6 Task 6 – PROVIDE emerging technology support (OPTIONAL)

The TIP Contractor shall establish and maintain a program for the enhancement and improvement of IT services, analyzing emerging technologies and transformative solutions. The TIP Contractor shall conduct an analysis every six (6) months. A written analysis and recommendations shall be provided to the TPOC, or COR within five (5) business days of completing the analysis. The TIP Contractor must base the analysis upon an assessment of the current information technology capabilities, evaluations of the operations efficiency of IT, considerations regarding the adequacy of information technology, market surveys of new and emerging technologies, and technological developments that could improve the cost effectiveness of the delivery of information technology services. For example, the TIP Contractor shall explore the advantages of desktop virtualization technology with regards to the DHS objectives and constraints. The TIP Contractor may propose alternative desktop solutions which deviate from the current desktop/laptop paradigm within DHS. The TIP Contractor shall also explore Multi-Level Security options for areas which process classified information as long as accreditable solutions exist. The level of effort supporting this task is estimated to not exceed ten (10) FTEs annually.

C.4.7 Task 7 – PROVIDE logistics support (OPTIONAL)

This Task is complementary to Task 4. There are two (2) primary distinctions between the two (2) tasks:

- Task 7 will support the transition of employees from their current location onto the Campus. Preparation for this move will start prior to the exercise of Task 4. Also, employees will move over the course of several months. All transition related support shall be performed under Task 7 – Logistics.
- Task 7 supports the TIP Contractor provided warehousing function during Phase 1 and Post Phase 1.

C.4.7.1 SUBTASK # 1 – TRANSITION

C.4.7.1.1 TRANSITION-IN

The TIP Contractor shall prepare and provide an initial Transition Plan. Once approved, the TIP Contractor shall update the Plan throughout for each subsequent phase. The Transition Plan shall present a methodology detailing how transition will occur as DHS employees move onto the Campus throughout the Task Order, and how transition will occur to either the Government or to another Contractor at the end of the Task Order. The transition activities shall ensure business continuity, minimizing interruption and degradation of service. The Transition Plan shall address, at a minimum, the following areas:

- Performing buy vs. move cost benefit analyses
- Establishing project plans for migration activities
- Identifying resources required for migration; performing migration activities; managing migration activities
- Performing gap analyses on as-is and to-be architectures
- Recommending migration approaches
- Taking measurements of performance before and after migration in areas such as customer satisfaction, service availability, and conducting comparisons
- Communicating, educating, and/or training support personnel and end users on impacts and issues related to changes resulting from transition activities
- Developing a move schedule (including the scheduling of loading docks from vacating locations) in coordination with the Campus Coordinator
- Holding meetings with the Campus Coordinator for the eight (8) weeks prior to the move
- Disconnecting all IT equipment to be moved and bag all cables, etc. and marking with a label the afternoon before the move
- Installing IT equipment immediately after completion of move

C.4.7.1.2 COMPLETION / TRANSITION OUT

At the completion of the final option period or upon receipt of notice to transition from the Government/notice to proceed for the new Contractor, the TIP Contractor shall implement its Transition-Out Plan no later than (NLT) ninety (90) calendar days prior to expiration of that period. The Transition-Out Plan shall facilitate a seamless transition from the incumbent to other designated incoming contractor. The TIP Contractor shall identify how they will coordinate with the incoming and/or Government personnel to transfer knowledge regarding the following:

- Project management processes

- Points of contact
- Location of technical and project management documentation
- Physical inventory
- Status of ongoing technical initiatives
- Appropriate Contractor-to-Contractor coordination to ensure a seamless transition.
- Identify schedules and milestones
- Identify actions required of the Government
- Establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition via weekly status meetings

C.4.7.2 SUBTASK # 2 – WAREHOUSING /ASSET MANAGEMENT

The TIP Contractor shall manage the procurement, receiving, asset inventory, deployment, refresh, disposal, warranties, and security of all assets within the Campus or scheduled to be transferred to the Campus, whether Government-owned or TIP Contractor-owned. The TIP Contractor shall perform the complete spectrum of asset management services, which shall include at a minimum:

- Providing an asset management capability to electronically and physically inventory assets, reveal configurations, and reconcile all pertinent information regarding IT resources in a comprehensive asset-tracking (CMDB) repository for the entire organization.
- Perform redeployment and disposal actions. This service shall include life cycle analysis to facilitate effective and efficient use of assets by assessing asset utilization, standardizing configurations, and preventing unneeded purchases.
- Store, inventory, asset tag, transport, maintain accountability, and deploy assets from a DHS approved TIP contractor warehouse facility, until the campus warehouse is complete.
- Integrating the asset management systems to the help desk application to allow operational IT technicians to quickly review vital aspects of a customer's computing environment.
- Tracking and updating all asset events and status changes such as installation, upgrades, movement between locations, user and organizational assignment, repair, maintenance, replacement events, and disposal. The TIP Contractor shall record these events in the DHS-provided asset management systems.
- All assets shall be recorded in Sunflower or other GFE that shall be electronically updated.
- Operating, updating, and maintaining the DHS asset management application and asset records to reflect configuration changes.
- Preparing and submitting asset reports to the TPOC.
- Managing, maintaining, and updating all required elements of the asset record, from asset acquisition throughout the asset's lifecycle up to and including decommissioning, in the prescribed asset management application.

- Updating and maintaining the asset management applications with the following information at minimum:
    - Accurate and up-to-date data for all required fields, including person assigned, physical location to include facility, building, floor and room, organization, Property Control Officer (PCO), and asset history.
    - Standardization of record formats to include a data dictionary with predefined definitions and acronyms used for record entries.
    - Inventory of application licenses and track the distribution of licenses.
    - Initial cost, incremental costs, and ownership status (purchase or lease).
    - Retain, reconfigure, and reissue serviceable surplus hardware.
    - Manufacturer information including name, model or version numbers, and serial number).
    - Acquisition information to include vendor, contract number, delivery order, date of purchase, date received, deployment date and any service dates.
    - Warranty information to include provider, expiration, and service standard.
    - Operating system and software release and/or patch version, date installed, and Government verification of installation (date and verifier).

Asset Receipt & Distribution

The TIP Contractor shall:

- Place the equipment into inventory and/or arrange delivery to the Customer and update the DHS asset record with assignment information after delivery. The TIP Contractor shall manage all inventory facilities and equipment issuance.
- Stage equipment prior to shipment for new installations to facilitate seamless systems operation and reduce maintenance costs.
- Reconcile asset delivery with acquisition notification, identify discrepancies between purchase orders and shipments, validate for payment and provide payment verification to designated contract support personnel, and resolve discrepancies. If the TIP Contractor finds a damaged shipment, then the TIP Contractor shall coordinate equipment repair/replacement with the vendor.
- Manage, maintain, and file asset records for all items in the approved asset management application regardless of administrative assignment of the asset.
- Receive notification of asset acquisition; coordinate delivery, receive the asset, apply DHS tag or USCG tag (if required) and enter asset information into the Government furnished asset management application.
- Notify the receiving Property Control Officer (PCO) of the delivery of the asset and update the asset-tracking application with the asset's assignment information to include organization, user, and PCO.
- Request and obtain monthly lists of all projected new and departing personnel from DHS and its associate contractors. These lists shall form basis for the activation/deactivation of accounts, asset reclamation/re-assignment actions, and updates to the asset assignment information in the Asset Management application.

Provide Spares Provisioning

The TIP Contractor shall:

- Prepare and maintain a Support Plan to govern spares management, the forward deployment of spares to maintenance support offices and DHS sites, the repair and replenishment actions, and status reporting.
- Maintain a stock of spare parts, based on Original Equipment Manufacturer (OEM) recommendation and failure analysis based on actual user tickets and reports. Demand will alter quantity stocked, including re-order point, buffer quantity, and order/ship time (OST) allowance. For stock control, the TIP Contractor shall use a stock control/Enterprise Resource Program capability. The TIP Contractor shall maintain the stock of GFE in sufficient quantity to fulfill performance standards in accordance with the PRS.
- The TIP Contractor procurement system shall provide linkage to DHS financial controls for stewardship surveillance.

Government Furnished Equipment Use/Re-Utilization Plan

The TIP Contractor shall develop, maintain, and update a GFE Use/Re-Utilization Plan for GFE use, re-utilization and disposition based upon an express set of guidelines detailing the structured analysis and disposition of the GFE hardware and software. The Plan shall include standards set by the system definition and design, and shall include the list of specifications the hardware and software must meet to qualify for use in the specific network or system. The Plan shall include guidelines that address the ability of the existing hardware and software to meet required DHS security requirements, and the compatibility of the existing applications and services with the system infrastructure. The Plan shall include a template for documenting the business case for the use/re-utilization of GFE versus new hardware, software, and circuits. Any re-utilization of Government applications assumes that the Government or the Government's designated Contractor shall modify, certify, and accredit the applications prior to integration. The Plan shall also include evaluation of, and beneficial alternative recommendations for, disposition of currently leased vendor equipment/property.

Decommission and Disposal

Upon identification and or notification that a hardware asset is to be decommissioned, the TIP Contractor shall perform the following actions:

- Arrange for retrieval of item
- Update asset record to reflect change in status
- Sanitize/degauss hard drive utilizing approved degaussing equipment specified in National Security Agency/Central Security Service Policy 9-12
- Prepare item for surplus, donation, or disposal
- Complete all documentation requirement for decommissioning
- Facilitate final disposition of hardware and software

Asset Accountability

The TIP Contractor shall conduct quarterly physical inventories of all IT hardware and software assets, software licenses, wireless devices, copiers, fax machines, telecommunications equipment, and any other designated accountable IT property, consistent with DHS policy. The TIP Contractor shall reconcile the findings of these physical inventories with the records maintained in DHS Sunflower.

The TIP Contractor shall provide a report on asset and software license utilization, configuration anomalies, and warranty status.

C.5 SECTION 508 COMPLIANCE

The TIP Contractor shall describe its approach for complying with Section 508 and conducting research to ensure that products and services comply with 36 CFR Part 1194 – Section 508 of the Rehabilitation Act (29 U.S.C. 794d).

Section 508 of the Rehabilitation Act requires Federal agencies to make their Electronic and Information Technology (EIT) accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use EIT. All EIT procured through this Task Order must meet the applicable accessibility standards specified in 36 CFR 1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this Task Order are listed below.

The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment.

Applicable Standards, which apply to this acquisition:

Section 1194.21: Software Applications and Operating Systems
Section 1194.22: Web-based Internet Information and Applications
Section 1194.23: Telecommunications Products
Section 1194.25: Self-Contained, Closed Products
Section 1194.26: Desktop and Portable Computers
Section 1194.31: Functional Performance Criteria

SECTION D – PACKAGING & MARKING

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section D of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING

The TIP Contractor shall deliver all electronic versions by email and CD-ROM, as well as by placing in the GSA PBS and/or DHS designated repository. Identified below are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text — Microsoft Word
- Spreadsheets — Microsoft Excel
- Briefings — Microsoft PowerPoint
- Drawings — Microsoft Visio
- Schedules — Microsoft Project

The TIP Contractor shall prepare all correspondence in and maintain all files using generally accepted commercial industry standards in accordance with the appropriate current National Archives and Record Administration (NARA) and General Records Schedule (36 Code of Federal Regulations (CFR) 122014 and 44 U.S.C. 3301). The website at http://www.archives.gov/records-mgmt/ardor/records-schedules.html contains the index of NARA schedules. All TIP Contractor files, records, and documents maintained in the performance of this Task Order are Government property, and the TIP Contractor shall return them upon completion or termination of the work. However, internal proprietary TIP Contractor business files are not Government property.

Document Management

For all deliverables within this Task Order, the TIP Contractor shall implement document management to include version control and comment resolution such that each release has clear inventory of comments accepted/rejected as part of the version.

SECTION E - INSPECTION AND ACCEPTANCE

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section E of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

E.2 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports and other deliverables under this Task Order shall be performed by the FEDSIM COR, with input from the GSA PBS and DHS TPOC(s).

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the Task Order. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period not to exceed 15 business days after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the TIP Contractor's proposal, and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the TIP Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper formatting, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the TIP Contractor for correction and resubmission. If the TIP Contractor requires additional Government guidance to produce an acceptable draft, the TIP Contractor shall arrange a meeting with the FEDSIM COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 work days (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the TIP Contractor shall have ten (10) business days to incorporate the Government's comments and/or change requests, and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Contracting Officer (CO)/Contracting Officer's Representative (COR) shall provide written notification of acceptance or rejection of all final deliverables within 15 business days unless specified otherwise in Section F. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the TIP Contractor, within ten (10) business days of the rejection notice. If the deficiencies cannot be corrected within ten (10) business days, the TIP Contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten (10) business days.

For FFP –

If the TIP Contractor does not provide products or services that conform to the requirements of this Task Order, the Government will not pay the fixed price associated with the non-conforming products or services.

For CPAF –

If the TIP Contractor does not provide products or services that conform to the requirements of this Task Order, the Government will document the issues associated with the non-conforming products or services in the award fee determination report and there will be an associated reduction in the earned award fee.

E.8 Inspection by Government Agencies

Per FAR 52.246-6, the TIP Contractor shall provide access to and cooperate with Government personnel conducting official inspections and surveys. Government personnel other than the CO or Quality Assurance Personnel may periodically observe TIP Contractor operations. However, the CO is the only person that may obligate the Government or direct TIP Contractor operations. The following list identifies agencies performing inspections:

- Quality Assurance Evaluators
- Property Inspectors
- The Inspector General (IG)
- Other offices in the DHS such as the Facilities and Services Department

- Other federal agencies such as the Occupational Safety and Health Administration (OSHA)
- Environmental Protection Agency (EPA)
- Government Accountability Office (GAO)
- General Services Administration (GSA)
- Defense Contracting Audit Agency (DCAA)
- DHS Office of Security

SECTION F – DELIVERABLES OR PERFORMANCE

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section F of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

F.3 PERIOD OF PERFORMANCE

The period of performance for this Task Order is from June 6, 2011 to June 5, 2018.

F.4 PLACE OF PERFORMANCE

Place of Performance is St. Elizabeths Campus, and any TIP Contractor support facilities in the metropolitan Washington, DC area. The TIP Contractor shall perform at the TIP Contractor's service desk location (CONUS).

F.5 DELIVERABLES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this Task Order.

The TIP Contractor shall notify the COR and TPOC when a deliverable is ready for review and provide the document online. The TIP Contractor shall post, store, and maintain all deliverables and all documentation produced pursuant to this Task Order on the DHS SharePoint Portal.

The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
Day: Calendar Day unless otherwise stated

SDR: System Design Review
CDR Critical Design Review
PDR Preliminary Design Review
PRR Production Readiness Review
IMS Integrated Master Schedule

The TIP Contractor shall deliver the deliverables listed in the following table:

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
1	Kickoff Meeting	C.4.1.1	Date of award plus 15 calendar days
2	Monthly Status Report	C.4.1.2	Monthly by the 10th business day of the month
3	Technical Status Meetings	C.4.1.4	As needed over the life of the Task Order
4	Status Meetings – Meeting Minutes	C.4.1.4	5 business days following the meeting

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
5	Program Management Plan (PMP) • Quality Management Plan (QMP) • Work Breakdown Structure • Earned Value Management Plan • Risk Management Plan • Configuration Management Plan	C.4.1.5	At Program Kickoff meeting
6	PMP – Updated	C.4.1.6	Yearly over the life of the Task Order
7	Reports and Analysis	C.4.5	As needed over the life of the Task Order
8	Written Analysis an Recommendations	C.4.6	Every 6 months over the life of the Task Order
9	Transition -In Plan	C.4.7.1.1	90 Calendar days prior to completion of Task 3 for each Phase
10	Transition-Out Plan	C.4.7.1.2	No later than 90 Calendar days prior to the expiration of each Phase
11	Prepare and submit asset reports to TPOC	C.4.7.2	As required
12	Asset Report	C.4.7.2	As required
13	Section 508 Product Accessibility Report	C.5	No later than 30 Calendar days after Task Order Award, as required
14	Section 508 National Security Exception Request and Authorization (DHS Form 4105)	C.5	As required
15	IT Security Plan	H.7.4.4	30 Calendar days after Task Order Award
	PHASE 1		
16	Integrated Baseline Review – Phase 1	C.4.1.3	145 Calendar days after Task Order award
17	Design Plan – Phase 1 Functional Requirements Document	C.4.2	Days following start of Phase : Preliminary at SDR; Final 15 business days after CDR
	Architectures (e.g., wireless, network, IBS)		Preliminary at SDR; Final 15 business days after CDR
	Detailed Engineering Design Plans (drawings, bill of materials, etc.)		Preliminary at PDR; Final 15 business days after CDR
	Desktop Image Management Plan		Preliminary at PDR; Final 15 business days after CDR
	Concept of Operations		Preliminary at SDR; Final 15 business days after CDR
	Requirements Traceability Matrix (RTM)		Preliminary at SDR; Final 15 business days after CDR
	Logical Design Document (Map to the		Preliminary at PDR; Final 15

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
	Business Architecture)		business days after CDR
	Master Service Agreement (MSA)		Preliminary at CDR; Final 15 business days after PRR
	Map to Technical Reference Model (TRM)		Preliminary at PDR; Final 15 business days after CDR
	Interconnect Security Agreement (ISA)		Preliminary at CDR; Final 15 business days after PRR
	Privacy Impact Assessment (PIA)		Preliminary at CDR; Final 15 business days after PRR
	Privacy Threshold Assessment (PTA)		Preliminary at SDR; Final 15 business days after CDR
	Section 508 EIT Accessibility Plan		Preliminary at CDR; Final 15 days after PRR
	System of Record Notification (SORN)		Preliminary at CDR; Final 15 business days after PRR
	Technology Insertion Decision Request		Preliminary at CDR; Final 15 business days after PRR
	Technology Refreshment/Evolution Plan		Preliminary at CDR; Final 15 business days after PRR
18	Test and Evaluation Master Plan (TEMP) – Phase 1	C.4.3	Preliminary at SDR; Final 15 business days after CDR
19	Development Test Plans	C.4.2	Preliminary at SDR; Final 15 business days after CDR
20	Operations and Maintenance Plan – Phase 1	C.4.4	Days following start of Phase:
	COOP		330 (Preliminary) 590 (Final)
	CONOPS		330 (Preliminary) 590 (Final)
	SLAs		330 (Preliminary) 590 (Final)
	SOPs		330 (Preliminary) 590 (Final)
	Training Plan(s)		330 (Preliminary) 590 (Final)
	Performance Reports		600 (Preliminary) 960 (Final)
	Pilot Results Report		600 (Preliminary) 960 (Final)
	C&A Updates (every 3 years or when major change is made)		600 (Preliminary) 960 (Final)
	Post Implementation Review (PIR) Results		600 (Preliminary) 960 (Final)
	Security Incident reports		600 (Preliminary) 960 (Final)
	DHS Periodic Reporting		600 (Preliminary) 960 (Final)
	FISMA metrics reports		600 (Preliminary) 960 (Final)
	FISMA Annual Assessment		As Required

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
	FISMA Metrics Reports		As Required
	Security Incident Reports		As Required
	SA Updates (every 3 years or when major change is made		As Required
	Lessons Learned		600 (Preliminary) 960 (Final)
	SLA Reports		600 (Preliminary) 960 (Final)
	Post Phase 1		
21	Integrated Baseline or IMS Review – Post Phase 1	C.4.1.3	Monthly
22	Design Plan – Post Phase 1 Requirement Definition and Analysis Architectures Systems Design Plan Detailed Engineering Design Plans (drawings, bill of materials, etc.) Desktop Image Management Plan Concept of Operations Requirements Traceability Matrix (RTM) Data Architecture Document (Map to the Data Architecture) Logical Design Document (Map to the Business Architecture) Enterprise Architecture (EA) Insertion Packages Master Service Agreement (MSA) Map to Technical Reference Model (TRM) Interconnect Security Agreement (ISA) Environmental Impact Statement (EIS) Historic preservation Assessment National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) Privacy Impact Assessment PIA) Privacy Threshold Assessment (PTA) Section 508 EIT Accessibility Plan Service Insertion Package (SIP) System of Record Notification (SORN) Technology Insertion Decision Request Technology Refreshment/Evolution Plan	C.4.2	Due NLT 15 business day prior to scheduled PDR, SDR and CDR design milestones as agreed to in the IMS. Consists of refreshed Phase 1 documents or new documents as required.
23	Comprehensive Test Plan – Post Phase 1	C.4.3	Refreshed Phase 1 documents or new documents as required, due at design review milestones, PDR, SDR and CDR
24	Certification and Accreditation Documentation	C.4.3	As required to meet production

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
	– Post Phase 1		(operational) ready target dates
25	Operations and Maintenance Plan – Post Phase 1 COOP CONOPS SLAs SOPs Training Plan(s) Performance Reports Pilot Results Report C&A Updates (every 3 years or when major change is made) Post Implementation Review (PIR) Results Privacy Documentation Security Incident reports DHS Periodic Reporting FISMA metrics reports Lessons Learned SLA Reports	C.4.4	Refreshed Phase 1 documents or new documents as required, draft due 90 business days and final due 30 business days prior to system production ready target date, or as agreed to in the IMS
	Contractor Proposed Deliverables For Phases 1 and Post Phase 1		
31	Configuration Management Plan	C.4.1.5	At Kickoff meeting
32	System Engineering Master Plan (SEMP). The SEMP is also a Subsidiary Plan in the PMP. • Includes the System Design Plan	C.4.1.5	At Program Kickoff meeting
33	System Security Plan (SSP)	C.4.3	As required to meet certification, accreditation and operational ready target dates
34	Security Requirements Traceability Matrix (SRTM)		
35	Security Risk Assessment (SRA)		
36	Security Test and Evaluation (ST&E) Plan		
37	Security Accreditation Package		
38	Plan of Action and Milestones (POA&M)		
39	Transition Plan System Acceptance Test Procedures Version Description Document (VDD) System Acceptance Test Report Section 508 Assistive Technology Interoperability Test Report Contingency Plan Critical Infrastructure Protection Report	C.4.7.1	Refreshed Phase 1 documents or new documents as required, draft due 90 business days and final due 30 business days prior to system

#	MILESTONE/DELIVERABLE	Task Reference	PLANNED COMPLETION DATE
	Disaster Recovery (DR Plan)		operational ready target date, or as agreed to in the IMS
	Operational Analyses		
	Quality Assurance Audit Reports (Transition)		
	Transition Design Intent Drawings (DID)		
	Transition Package		
	Operators Manuals		
	Maintenance Manuals		
40	Implementation Plan (Includes the GFE Use/Re-Utilization Plan)		Refreshed Phase 1 documents or new documents as required, draft due 90 business days and final due 30 business days prior to system operational ready target date, or as agreed to in the IMS

F.6 PLACE(s) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the Contracting Officer (CO) and/or Contracting Officer's Representative (COR) at the address below:

GSA FAS AAS FEDSIM

Gregory Lee, CO
GSA FAS AAS FEDSIM
1800 F Street, NW, 3100
Washington, DC 20405
Telephone: (202) 357-5831
Email: greg.lee@gsa.gov

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT

The TIP Contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) as soon as it becomes apparent to the TIP Contractor that a scheduled delivery will be late. The TIP Contractor shall include the rationale for late delivery in the PNR, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the TIP Contractor. Such notification in no way limits any Government contractual rights or remedies, including but not limited to termination.

SECTION H – SPECIAL ORDER REQUIREMENTS

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section G of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

G.3.5 CONTRACTING OFFICER'S REPRESENTATIVE

The Contracting Officer will appoint a Contracting Officer's Representative (COR) in writing for the Task Order. The COR will receive, for the Government, all work called for by the Task Order and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to TIP Contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the Task Order. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the Task Order.

G.9.6 INVOICE SUBMISSION

The TIP Contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the data elements indicated below shall be included on each invoice.

Task Order number:	GST0011AJ002*)*
Paying Number:	*(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project No.:	11024HSM (non ARRA),11030HSV (ARRA), 13032HSM and 13027HSM
Project Title:	DHS TIP

The TIP Contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The TIP Contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The TIP Contractor shall submit invoices as follows:

The TIP Contractor shall utilize FEDSIM's electronic Central Invoice Service (CIS) to submit invoices. The TIP Contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov/web/guest

The AAS Business Systems Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the TIP Contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.9.6.1 INVOICE REQUIREMENTS

The TIP Contractor may invoice the fixed fee on a monthly basis. The monthly fixed fee invoiced shall be proportionate to the amount of labor expended for the month invoiced.

The TIP Contractor shall submit simultaneous copies of the invoice to both GSA and the DHS POC.

If the Task Order has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six (6) months of project completion.

G.9.6.1.1 COST PLUS AWARD FEE (CPAF) CLINS (for LABOR)

The TIP Contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by TIP Contractor employee, and shall be provided for the current billing month and in total from project inception to date. The TIP Contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Monthly and total cumulative hours worked
- Billing rate
- Corresponding TO ceiling rate
- Cost incurred not billed
- Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the Contractor shall also include total Overhead Charges and General and Administrative Charges and shall also include the OH and G&A rate being applied.

The Government will promptly make payment of any award fee upon the submission, by the TIP Contractor to the FEDSIM Contracting Officer's Representative (COR), of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without issuing a Task Order modification if funds have been obligated for the award fee amount. The TIP Contractor shall attach the AFDO/CO determination letter to the public voucher and/or invoice.

G.9.6.1.2 COST PLUS FIXED FEE (CPFF) CLINS (for LABOR)

The TIP Contractor may invoice monthly on the basis of cost incurred for the CPFF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number

and title. All hours and costs shall be reported by CLIN element (as shown in Section B) and by TIP Contractor employee, and shall be provided for the current billing month and in total from project inception to date. The TIP Contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Monthly and total cumulative hours worked
- Billing rate
- Corresponding TO ceiling rate
- Cost incurred not billed
- Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the Contractor shall also include total Overhead Charges and General and Administrative Charges and shall also include the OH and G&A rate being applied.

G.9.6.1.3 FIRM FIXED PRICE (FFP) CLINS

The TIP Contractor may invoice as stated in Section B for the FFP CLINs. The invoice shall include the period of performance/deliverable or progress payment period covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element (as shown in Section B) and shall be provided for the current invoice and in total from project inception to date. The TIP Contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Firm Fixed Price (period of performance/deliverable or progress payment period – as stated in Section B)

G.9.6.1.4 TOOLS AND OTHER DIRECT COSTS (ODCs)

The TIP Contractor may invoice monthly on the basis of cost incurred for the tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and IA number. In addition, the TIP Contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- Tool/ODCs purchased
- Consent to Purchase number or identifier
- Date accepted by the Government
- Associated CLIN
- Project to date totals by CLIN
- Cost incurred not billed

- Remaining balance of the CLIN

All cost presentations provided by the TIP Contractor shall also include Overhead Charges, General and Administrative Charges and FPRA.

G.9.6.1.5 LONG DISTANCE TRAVEL

The contractor may invoice monthly on the basis of cost incurred for cost of long distance travel comparable with the JTR/FTR. Long distance travel is defined as travel over 75 miles outside of the St. Elizabeths Campus. The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA Account number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel detail shall include separate columns and totals and include the following:

- Travel Authorization Request number or identifier
- Current invoice period
- Names of persons traveling
- Number of travel days
- Dates of travel
- Number of days per diem charged
- Per diem rate used
- Total per diem charged
- Transportation costs
- Total charges

All cost presentations provided by the TIP Contractor shall also include Overhead Charges and General and Administrative Charges.

G.10 CONTRACT ADMINISTRATION

Contracting Officer:

Gregory Lee, CO
GSA FAS AAS FEDSIM
1800 F Street, NW, 3100
Washington, DC 20405
Telephone: (202) 357-5831
Email: greg.lee@gsa.gov

Contracting Officer's Representative (COR):

Dustin Dunn
GSA FAS AAS FEDSIM
1800 F Street, N.W.
Washington, D.C. 20405
Telephone: (202) 304-4745
Email: dustin.dunn@gsa.gov

Technical Point of Contact (TPOC) – DHS:

Kevin Sullivan
DHS/CRSO/OS
2701 Martin Luther King Ave SE, Washington, DC 20032
Phone: 202-561-4904
Email: kevin.sullivan@hq.dhs.gov

Technical Point of Contact (TPOC) - U.S. Coast Guard

LCDR Dana Schulman
U.S. Coast Guard Base National Capital Region
Attn: C4IT Department Stop 7118
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7118
Telephone: 202.372.4006
Email: dana.e.schulman@uscg.mil

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section H of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

H.2 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "key." The TIP Contractor shall propose appropriate labor categories for these positions. The Government does not intend to dictate the composition of the ideal team to perform this Task Order. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror.

Minimum security clearance standards are listed per Key Personnel description. During performance, Key Personnel clearance requirements will increase to the corresponding requirements for the physical security as it becomes accredited.

- Program Manager
- Deputy Program Manager
- Senior Network Architect
- Information Assurance Engineering Lead

- Physical Security Lead
- Intelligent Building Systems Lead
- Audio/Visual Lead
- Operations & Maintenance (O&M) Lead
- Real Time Engineering Services Lead

The Government desires that Key Personnel be assigned for the duration of the Task Order.

H.2.1 PROGRAM MANAGER

The TIP Contractor shall identify a Program Manager (PM) to serve as the Government's single point of contact and to provide overall leadership and guidance for all TIP Contractor personnel assigned to the Task Order. The PM is ultimately responsible for the quality and efficiency of the Task Order to include both technical issues and business processes. The PM shall be an employee of the prime Alliant TIP Contractor. The PM shall assign tasking to TIP Contractor personnel, supervise on-going technical efforts, and manage overall Task Order performance. This individual shall have the ultimate authority to commit the TIP Contractor's organization and make decisions for the TIP Contractor's organization in response to Government issues, concerns, or problems.

It is required that the Program Manager possess the following security clearance and certifications:

- Certifications: PMI PMP Certified, ITIL Version 3 Foundations Certified (minimum).
- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the Program Manager possess the following experience and qualifications:

- Experience in planning, directing, and managing complex IT programs of a nature similar in size and scope of this Task Order.
- Knowledge and experience in systems/infrastructure implementation in a campus construction environment.
- Experience with the management and supervision of a significant number of multi-disciplinary staff (100 persons or more) of various labor categories and skills in projects similar in size and scope as proposed for this Task Order.
- Demonstrated written and oral communication skills, including experience in presenting material to senior Government officials.

H.2.2 DEPUTY PROGRAM MANAGER

The TIP Contractor shall identify a Deputy Program Manager (DPM) to serve as the Government's single-point-of-contact in the absence of the Program Manager and to provide leadership and guidance for all TIP Contractor personnel assigned to the Task Order. The deputy

PM shall assign tasking to TIP Contractor personnel, supervise on-going technical efforts, and manage overall Task Order performance in the absence of the PM. This person shall be readily available in the absence of the PM to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues.

It is required that the Deputy Program Manager possess the following security clearance and certifications:

- Certifications: PMI PMP Certified, ITIL Version 3 Expert Level Certified (minimum).
- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the Deputy Program Manager possess the following experience and qualifications:

- Experience in planning, directing, and managing complex information technology programs of a nature similar in size and scope of this Task Order .
- Knowledge and experience in systems/infrastructure implementation in a construction environment.
- Experience with the management and supervision of a significant number of multi-disciplinary staff (100 persons or more) of various labor categories and skills in projects similar in size and scope as proposed for this Task Order.
- Demonstrated written and oral communication skills, including experience in presenting material to senior Government officials.

H.2.3 SENIOR NETWORK ARCHITECT

The TIP Contractor shall identify a Senior Network Architect to be the lead for systems engineering and integration as well as enterprise architecture planning and design.
It is required that the Senior Network Architect possess the following security clearance and knowledge:

- Knowledge of Packet-Optical Transport Platform (P-OTP) and Passive Optical Network Technologies.
- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the Senior Network Architect possess the following experience and qualifications:

- In-depth experience and knowledge in Systems Engineering best practices and methodologies.

- Knowledge of all the underlying technologies listed in the Performance Work Statement and the proven ability to integrate all the technologies, systems and services over a common infrastructure.
- Experience in enterprise architecture planning and design in the context of Federal Government enterprise architecture standards.
- Demonstrated written and oral communication skills, including experience in presenting material to senior Government officials.

H.2.4 INFORMATION ASSURANCE ENGINEERINGING LEAD

It is required that the Information Assurance Engineering Lead possess the following security clearance and certifications:

- A Level 3, DOD 8570 Certification .
- Security Clearance Requirement: TS SCI at time of proposal.

It is desired that the Information Assurance Engineering Lead possess the following experience and qualifications:

- Experience in planning, directing, and managing complex information assurance projects/operations of a nature similar in size and scope of this Task Order.
- Knowledge of NIST, DIACAP, and DHS certification and accreditation concepts and procedures of this Task Order.
- Knowledge of network and system operations, to include OSI multi-layer network and system security risk mitigation strategies.
- Knowledge of Type 1 encryption devices and procedures as they relate to classified networks.
- Knowledge of current ITIL process version 3 frameworks.

H.2.5 PHYSICAL SECURITY LEAD

It is required that the Physical Security Lead possess the following security clearance:

- Security Clearance Requirement: TS SCI at time of proposal.

It is desired that the Physical Security Lead possess the following experience and qualifications:

- Demonstrated experience designing and performing in Interagency Security Committee Level 5 environment.
- Knowledge of certification and accreditation concepts and procedures as required by the Director of Central Intelligence Directives (DCID) 6/9 and ICD-705 of this Task Order.
- Documented experience with Underwriters Laboratories UL-2050 and UL-1981.
- Knowledge of physical security network and system operation design to include:
    - security access control
    - video assessment

- high-end intrusion detection
- video switching systems
- electronic surveillance
- intrusion detection
- annunciating systems

H.2.7 AUDIO/VISUAL (A/V) LEAD

The TIP Contractor shall identify an A/V Lead who will be the TIP Contractor's lead for planning, design, and implementation of A/V technology.

It is required that the A/V Lead possess the following security clearance:

- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the A/V Lead possess the following experience and qualifications:

- Experience designing and deploying Government and DoD multi-media display systems, video teleconferencing including encryption and secure.
- Experience designing and deploying auditorium and production interface, TV and broadcast news requirements, content management, and subscriber management systems and acoustic and video display systems.
- Experience in gathering requirements, implementing new technologies, and designs in a Government environment.
- Demonstrated written and oral communication skills, including experience in presenting material to senior Government officials.

H.2.8 OPERATIONS & MAINTENANCE (O&M) LEAD

It is required that the O&M Lead possess the following security clearance and certifications:

- Certifications: PMI PMP Certified, ITIL Version 3 Intermediate Level Certified (minimum).
- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the O&M Lead possess the following experience and qualifications:

- Demonstrated experience planning the transition and integration of several thousand employees to a multi-building Campus.
- Design of an integrated and unified network management, service desk, portfolio asset management, and incident response system.

- Establishing performance metrics, implementing service level agreements, and meeting/exceeding measures.

H.2.9 REAL-TIME SERVICES TELECOMMUNICATIONS ENGINEERING LEAD

The TIP Contractor shall identify a Real-Time Services Telecommunications Engineering Lead who will be the TIP Contractor's lead for the planning, designing, and implementing of all voice, video, and data real-time services over the DHS TIP Campus infrastructure. The Real-Time Services Telecommunications Engineering Lead is required to possess the following security clearance:

- Security Clearance Requirement: Department of Defense (DOD) Defense Security Service (DSS) and/or Office of Personnel Management (OPM) Single Scope Background Investigation (SSBI).

It is desired that the Real-Time Services Telecommunications Engineering Lead possess the following experience and qualifications:

- Experience in the design and integration of real-time voice, video, and data services, to include the underlying technical performance issues and solutions, protocols, and Components required to transport these real-time services across a Campus and wide area network infrastructure.
- Experience in designing a Campus wide VoIP system to the requirements set forth in the Joint Interoperability Testing Command (JITC) Unified Capability Requirements (UCR) 2008 Change 1 or 2 Document.
- Experience with designing, integrating, and deploying real-time services and enterprise telecommunications of a similar size and scope to this Task Order.
- Experience with traditional TDM systems and circuits, wireless telecommunications, and capacity planning.

H.2.11 KEY PERSONNEL SUBSTITUTION

The TIP Contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to the Task Order Request, the TIP Contractor shall notify the Government CO and the COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s) in sufficient detail to permit evaluation of the impact on Task Order performance.

Substitute personnel qualifications shall be equal to or greater than those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the Task Order, the TIP Contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

H.2.12 NON KEY PERSONNEL

The impact of any changes to non-Key Personnel shall be that the qualifications of the team remains equal or better to the original proposed team.

A registered communication distribution designer (RCDD) shall be assigned to the project and available as required. The RCDD will be the TIP Contractors registration authority for the communications low voltage cabling design and installation.

H.5 GOVERNMENT FURNISHED PROPERTY (GFP), SERVICES (GFS), EQUIPMENT (GFE), AND INFORMATION (GFI)

H.5.1 GOVERNMENT FURNISHED PROPERTY (GFP)

Government Furnished Property (GFP) is applicable to the performance of this Task Order. The TIP Contractor is authorized to use GFP at the Campus for the duration of this Task Order in accordance with the requirements of this Task Order. This Section describes the property and services the Government will furnish to the TIP Contractor for performance of the requirements of this Contract. The Government will provide to the TIP Contractor the following access for use: (1) Government Furnished Property (GFP) for which the contractor is responsible and accountable; and (2) property only made available to the contractor, as listed below in this section. The TIP Contractor shall take all reasonable precautions and such other actions as may be directed by the Government, or in the absence of such direction, in accordance with sound business practice to safeguard and protect Government property in the contractor's possession or custody listed in this section. The TIP Contractor shall accept Government-provided automated information systems (AIS) hardware and software without exception. Government Furnished Equipment (GFE) may include Government-leased equipment or Government-owned equipment. The TIP Contractor shall not use GFP or services for any other purpose than those described in this Task Order. The TIP Contractor shall not remove GFP from DHS facilities or other supported areas without review and written approval of the CO or authorized representative. The provisions affecting GFP under this section shall be IAW FAR 52.245-5. The Government may direct the TIP Contractor to develop and /or revise milestones for joint inventory and transfer of GFP.

All Government furnished property shall remain the property of the Government and shall be returned to the Government prior to the end of this Task Order. In addition, any Government furnished information provided shall not be shared unless written approval is obtained from the Government, in advance of sharing Government furnished information. Any TIP Contractor contributions to Government furnished information under this Contract shall become the property of the Government.

The contractor shall not mark or affix any decals, emblems or signs portraying the contractor's name or logo to Government Equipment, Facilities, or Property except as directed by the TPOC.

H.5.1.1 PRIOR TO PHASE 1 OCCUPANCY

Prior to Phase 1 occupancy of the Campus, the Government will not provide standard office space as Government Furnished Property (GFP) for TIP Contractor personnel on the St.

Elizabeths campus or at any other location. The TIP Contractor shall provide a Temporary Construction Facility (i.e., a trailer), furniture, associated office supplies and equipment, and connections (electrical, plumbing, etc.) which the TIP Contractor shall pay for. The Government will provide telephones, telephone communication service, desktop computers or laptops with associated equipment, and network access for conducting official business in the performance of this Contract.

The Government will grant access to DHS applications and data on an as-needed basis upon request by the TIP Contractor.

H.5.1.2 OCCUPANCY

During occupancy, limited facilities will be made available to the TIP Contractor to support occupants and operations centers. The Temporary Construction Facility referenced above shall remain the TIP Contractors primary facility for unoccupied future phase buildings and development. For occupied Campus zones, the Government shall provide, without cost to the contractor, facilities (office space with desk and chair), equipment (computer, access to printer, copier, and fax), materials (all related office supplies), and/or other services necessary to perform the requirements in the Operations and Maintenance, task 4.

H.5.2 GOVERNMENT FURNISHED SERVICES (GFS)

H.5.2.1 TELEPHONE SERVICE

The Government will furnish telephone service at TIP Contractor-occupied Government sites to include local and long-distance calls.

The TIP Contractor shall comply with DHS rules and regulations regarding telephone use.

The TIP Contractor shall obtain prior Government review and written approval before connecting or disconnecting any Contractor Furnished Equipment (CFE) to Government-furnished communications systems or equipment.

H.5.2.2 Local Area Network (LAN)

The Government will provide limited access to the existing LAN at contractor-occupied Government facilities to include E-Mail capability. The TIP Contractor shall not use the LAN for purposes other than for work required under this Task Order.

Paper Products: The Government will make available containers in shared Government facilities for the collection of recyclable paper.

H.5.2.3 Reporting Discrepancies in Performance of Government Furnished Service Contracts

The TIP Contractor shall report discrepancies in performance of Government-provided services to the CO and TPOC (CDRL C.3.1-1, Government Furnished Service Discrepancy Report).

H.5.3 GOVERNMENT FURNISHED EQUIPMENT (GFE)

The Government will provide GFE (such as telecommunications, computers, network components, storage devices, software, and peripherals) to the TIP Contractor to complete the duties of this Task Order with the exception of equipment for the Help Desk and unclassified Test Lab.

H.5.3.1 EQUIPMENT OFFERED FOR CONTRACTOR USE

The Government will furnish Original Equipment Manufacturer (OEM) Software. The result of the last inventory of equipment in the metropolitan Washington D.C. area and other select locations will be provided.

H.5.3.2 CONTRACTOR ACCOUNTABILITY

Transfer of Accountability: The TIP Contractor shall become accountable for GFE when assigned.

Property Administration: The TIP Contractor shall perform property administration in accordance with FAR Part 45.

Report of Government Property: The TIP Contractor shall prepare and submit to the TPOC an annual Report of Government Property as directed by the TPOC (CDRL C.3.1-2, Government Property Report – Annual).

Turn-In of GFE: The TIP Contractor shall prepare a recommendation for excess when GFE is no longer required or suitable for its intended use, or has reached the end of its technical life. The contractor shall provide these recommendations to the DHS TPOC who will make the final determination of the disposition of the equipment. The TIP Contractor shall process the items in accordance with applicable Federal regulations, and Department of Homeland Security policies and regulations. All Government furnished property and IT equipment identified in this Task Order shall remain the property of the Government.

Replacement of GFE: The TIP Contractor shall coordinate with the DHS TPOC for replacement of GFE. Upon approval by the DHS TPOC, the item(s) of equipment to be replaced will be deleted from the GFE listing. If required to maintain performance standards, the Government will provide comparable GFE replacement. The TIP Contractor shall contact the Help Desk for problems regarding computers and peripherals. The Government will replace computers and peripherals.

H.5.3.3 INITIAL INVENTORY ASSESSMENT AND ACCOUNTABILITY

Initial Inventory Procedures: The TIP Contractor shall attend a phase-in GFP transfer and inventory meeting with the Government. The TPOC will schedule the meeting prior to performance period start date.

The TIP Contractor shall conduct a phase-in 100% joint inventory within ten (10) business days of Task Order start date. This inventory shall verify access to items such as facilities, to include keys; property received from the designated property control officers; and materiel items of work in progress; e.g., items in various stages of repair. This provision does not preclude prior inspection of GFP by the contractor. The operational or conditional status of all GFF and on-site GFE shall be determined during the joint inventory. The TIP Contractor shall record any item found to be broken or not suitable for its intended purpose. The DHS TPOC and the TIP Contractor shall certify as accurate the joint inventory. The TIP Contractor shall keep the inventory listing current. Initial GFP is minimal.

The TIP Contractor and the TPOC shall jointly inspect all GFE at the time of the inventory. The TIP Contractor shall note all valid discrepancies, and the Government may correct the discrepancies by one or more of the following methods at the Government's option. The

Government may elect not to provide equipment to the contractor; or may correct noted discrepancies prior to performance period start date; or may require the contractor to repair discrepancies subject to reimbursement by the Government. The TPOC will determine validity.

Withdrawal of GFE: The Government retains the right to withdraw any GFE at any time during the performance of the Task Order. When possible, the Government will provide at least 30 business days notice of the impending withdrawal of GFE when deemed necessary or appropriate.

Equipment and Software Manuals: After conducting a joint inventory, the Government will turn over to the contractor equipment operating manuals presently maintained by the Government. The TIP Contractor shall update these documents as new issues are published. Updated manuals are the property of the Government upon completion or termination of this Task Order.

H.5.4 GOVERNMENT FURNISHED INFORMATION (GFI)

Government Furnished Information is provided in Section J.

H.5.4.1 GFI – DATA RIGHTS

In addition, all data collected by the TIP Contractor are the property of the Government and shall be considered GFI, as defined herein. All data collected by the TIP Contractor or provided to the TIP Contractor in the performance of this contract are the property of the Government. The Government retains all rights to the data used and all derivative works developed by the TIP Contractor. The TIP Contractor agrees that during performance of the contract and for a period of six (6) years after the completion of performance of this contract, the TIP Contractor, including all divisions thereof, and any affiliate of the TIP Contractor, any joint venture involving the TIP Contractor, any entity into or with which it may subsequently merge or affiliate, or any other successor or assign of the TIP Contractor, shall not:

Supply information or material received from this Task Order, to the public, or to any firm participating in or having a known prospective interest in the subject matter areas for which the sensitive information such as the name or mission of the Government agency/department that provided the data was initially submitted.

H.5.4.2 DHS MANAGEMENT DIRECTIVES

The following DHS Management Directives are applicable:

- 0002 - Operational Integration Staff
- 0003 - Acquisition Line of Business Integration and Management
- 0004 - Administrative Services Line of Business Integration and Management
- 0005 - Financial Management Line of Business Integration and Management
- 0006 - Human Capital Line of Business Integration and Management
- 0007.1 - Information Technology Integration and Management

- 0475 - Information Collection Program
- 0480.1 - Ethics-Standards of Conduct
- 0490.1 - Federal Register Notices and Rules
- 0560 - Real Property Management Program
- 0565 - Personal Property Management Directive
- 0590 - Mail Management Program
- 0731 - Strategically Sourced Commodities Policy and Procedures
- 0760.1 - Purchase Card Program
- 0782 - Acquisition Certification Requirements for Program Manager
- 0783 - Ordering Official Certification
- 0784 - Acquisition Oversight Program
- 1120 - Capitalization and Inventory of Personal Property
- 1130.1 - Electronic Funds Transfer for Disbursements, Collections and Deposits
- 1190.1 - Billings and Collections
- 1210.1 - Vendor Maintenance
- 1330 - Planning, Programming, Budgeting and Execution
- 1400 - Investment Review Process
- 1510.1 - Travel for Official Government Business
- 1560.2 - Payment of Official Travel Expenses by Non-Federal Sources
- 3120.2 - Employment of Non-Citizens
- 4010.2 - Appendix A- Software Applications and Operating Systems
- 4010.2 - Appendix B- Web-Based Intranet and Internet Information and Applications
- 4010.2 - Appendix C- Telecommunications Products
- 4010.2 - Appendix D- Video and Multimedia Products
- 4010.2 - Appendix E- Self-contained, Closed Products
- 4010.2 - Appendix F- Desktop and Portable Computers
- 4010.2 - Appendix G- Functional Performance Criteria
- 4010.2 - Appendix H- Information, Documentation and Support
- 4010.2 - Section 508 Program Management Office and Electronic and Information Technology Accessibility
- 4030 - Geospatial Management Office
- 4100.1 - Wireless Management Office
- 4200.1 - Guide to Information Technology Capital Planning & Investment Control (v7.1)
- 4200.1 - IT Capital Planning and Investment Control (CPIC) & Portfolio Management
- 4400.1 - DHS Web (Internet, Intranet, & Extranet Information) & Information Systems
- 4500.1 - DHS E-Mail Usage
- 4600.1 - Personal Use of Government Office Equipment
- 4700.1 - Personal Communications Device Distribution
- 4800 - Telecommunications Operations
- 4800 - Attachment A- Frequently Asked Questions (FAQs)
- 4800 - Attachment B- Logon Screen
- 4900 - Individual Use and Operation of DHS Information Systems-Computers
- 5110 - Environmental Compliance

- 8200.1 - Information Quality
- 9300.1 - Continuity of Operations Programs and Continuity of Government Functions
- 11005 - Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- 11020.1 - Issuance of Access Control Media
- 11021 - Portable Electronic Devices in SCI Facilities
- 11030.1 - Physical Protection of Facilities and Real Property
- 11041 - Protection of Classified National Security Information Program Management
- 11043 - Sensitive Compartmented Information Program Management
- 11044 - Protection of Classified National Security Information Classification Management
- 11045 - Protection of Classified National Security Information-Accountability, Control, and Storage
- 11046 - Open Storage Area Standards for Collateral Classified Information
- 11047 - Protection of Classified National Security Information Transmission and Transportation
- 11048 - Suspension, Denial and Revocation of Access to Classified Information
- 11049 - Protection of Classified National Security Information- Security Violations and Infractions
- 11050.2 - Personnel Security and Suitability Program
- 11051 - Department of Homeland Security SCIF Escort Procedures
- 11052 - Internal Security Program
- 11053 - Security Education, Training, and Awareness Program Directive
- 11056.1 - Sensitive Security Information (SSI)
- 11060.1 - Operations Security Program
- 11080 - Security Line of Business Integration and Management
- DHS SCG OS 001 HSDN J-6A (FOUO)
- DHS SCG OS 002 IT CA Final J-6B (FOUO)
- DHS Form 560-1
- DHS Form 560-3 Property Transfer Receipt
- 025-01 - Sustainable Practices
- 066-01 - Safety and Health Programs (Revision 00)
- 141-01 - Records Management
- 252-01 - Organization of the Department of Homeland Security (Revision 00)
- Homeland Security Acquisition Regulations (HSAR)

H.7 SECURITY REQUIREMENTS

Interim clearances are not permitted. All security clearances must be fully adjudicated and approved. All TIP Contractor personnel working on the DHS Secret Network (e.g., HSDN) shall possess a minimum of a SECRET clearance. All TIP Contractor personnel working on Top Secret Network (e.g., C-LAN) shall possess a fully adjudicated and approved TS/SCI clearance. It shall be the responsibility of the TIP Contractor to initiate reinvestigations of these persons through the Office of Personnel Management (OPM).

All Key Personnel are required to have a current fully adjudicated and approved required clearances, identified in Section H.2, and access at proposal due date. All personnel who will be working at sites within Sensitive Compartmented Information Facilities (SCIF), for activities other than installation and periodic maintenance, shall possess a fully adjudicated and approved TS/SCI clearance and access. The Government anticipates that the number of such personnel could approach 50% to 80% of the contractor technical personnel over the term of the Task Order.

COMSEC personnel are required to have a fully adjudicated and approved TS clearance with eligibility for SCI access.

Additional details will be specified in a Department of Defense (DOD) DD Form 254 in Attachment G.

H.7.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12)

DHS HSPD-12 identification cards will be used for physical, technical, and personal authentication for the Campus and management of access to facilities, networks, devices, and anything that requires authentication and controlled access. The DHS issued HSPD-12 cards must support all DHS Components, to include .mil network access. The TIP Contractor shall provide a list of TIP Contractor personnel that require DHS badges and security clearances. The Government will process background investigations and/or security clearances for the contractor staff to occur after submission of the staff listing, provided that the individuals meet the necessary security qualifications. The Government may grant approved TIP Contractor personnel temporary access to the St. Elizabeths site, subject to compliance with security and safety requirements, within 30 days of Task Order award. This does not provide access to any DHS accounts, systems, or locations. Upon successful adjudication of security clearances, access to DHS accounts, systems, and/or locations will be authorized. DHS will not perform security background investigations for staff that do not currently possess a Federal Secret, TS, or TS/SCI clearance.

H.7.2 POST AWARD SECURITY REQUIREMENTS

Prior to performing work on this contract, Contractor employees must complete the following two steps.

- Complete a CHQ Security Background Investigation and be granted a 90 day St. Elizabeths access approval.
- Begin the process of obtaining a favorable DHS Entry-on-Duty (EOD) status by submitting a DHS Form 11000.25 - Contract Suitability/Security Screening Request Form to the DHS TIP PMO for review and receive notification from the DHS TPOC that the form was sent to the DHS Office of Security, Personnel Security Division (PSD).

EOD must be achieved within the 90 day period or prior to accessing any DHS Information, Technology, Resources, or Systems, whichever comes first. Delays in achieving EOD caused by

the government will be considered for grace period extension if the 90 day grace period expires. Request for grace period extension due to delays not caused by the government will not be considered. It is the Contractor employee's responsibility to complete and submit information for the EOD process in a timely fashion.

The Government, on a limited basis, may waive the DHS EOD requirements for Contractor Employees based on the activities to be performed (e.g. cable installation, construction activities, or other duties where an individual would NOT need IT accounts nor access to secured areas).

Contractor employees performing installations and or periodic maintenance, without an adjudicated and approved DHS EOD, will require an escort with an approved DHS EOD and required security clearances and shall be provided by the Contractor. The escort ratio shall not exceed a 1 to 5 ratio (1:5), with escorted Contractor employees being within visual range of the escort at all times.

All Contractor employees without an adjudicated and approved DHS EOD who require access to the St. Elizabeths Campus shall submit, at least 3 Business Days (i.e., Monday - Friday) prior to the visit, a Visitor's Request to the St. Elizabeths Security Office. Access to the St. Elizabeths Campus will be granted upon adjudication and approval of the Visitor's Request.

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

- PSD receives Contractor employee's DHS Form 11000.25, "Contract Suitability/Security Screening Request"
- PSD sends Contractor employee email advising of their initiation into the electronic Standard Form 85P, "Questionnaire for Public Trust Positions" (The Standard Form (SF) 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM.) There is a 14 calendar day period for completion of this form.

After completion of SF 85P, PSD will send Contractor employee email requesting completion of the following forms.

- FD Form 258, "Fingerprint Card" (two copies)
- DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

It is the Contractor employee's obligation to complete these forms in a timely fashion. Only complete packages will be accepted by the DHS Office of Security/PSD for consideration of granting an EOD status to the Contractor employee. Specific instructions on submission of packages will be provided upon award of the Task Order.

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the Government do not relieve a contractor from performing under the terms of the Task Order.

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the TIP Contractor employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information, at any time during the term of the task order. No employee of the TIP Contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The TIP Contractor shall return to the Client Representative all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the Client Representative, referencing the pass or card number, name of individual to who it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on DHS telecommunications and automated information systems, the TIP Contractor shall provide for the administrative control of sensitive data being processed. TIP Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

TIP Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).
DHS Security Office POC Information:

Office of Security/PSD
Customer Service Support
Washington DC 20528
Telephone: (202) 447-5010

H.7.3 SECURITY AWARENESS TRAINING

The contractor shall be responsible for ensuring that all assigned contractor employees have received up-to-date DHS IT Security Awareness Training. Each contractor employee shall undergo refresher IT Security Awareness Training on at least an annual basis. All IT Security Awareness Training is provided monthly by the DHS Security Office. The contractor shall be

able to provide DHS with proof-of-training for each contractor employee. "Proof-of-training" is defined as the DHS-issued training certificate of successful course completion.

DHS reserves the right to assess the IT Security Awareness Training each contractor employee has taken (or will be taking) and to require alternative and/or additional training should the existing training content be deemed inadequate or irrelevant.

The contractor shall ensure that its personnel designing, programming, operating, using, or managing DHS systems/network and/or data in performance of the contract, are properly trained and must receive training at least annually in IT security awareness and security practices, policies, and procedures as required under the Computer Security Act of 1987 and OMB Circular A-130, including Appendix III.

The Contractor shall provide a report on an annual basis that shows that TIP Contractor personnel working on the contract have successfully completed all required IT security training, and that they are aware of their IT security responsibilities.

DHS reserves the right to assess the IT Security Awareness Training each TIP Contractor employee has taken (or will be taking), and to require alternative and/or additional training should the existing training content be deemed inadequate or irrelevant.

H.7.4 SECURITY COMPLIANCE REQUIREMENTS

H.7.4.1 COMPLIANCE WITH DHS SECURITY POLICY

All Sensitive but Unclassified (SBU) systems employed by this task must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook in Attachment H. All TIP Contractor systems used to process sensitive DHS data must be accredited for that use.

In addition, all national security systems produced by this task order must be compliant with DHS 4300B DHS National Security System Policy and the DHS 4300B National Security System Handbook Attachment I.

All encryption shall be Federal Industry Processing Standards (FIPS) 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

H.7.4.2 ACCESS TO UNCLASSIFIED FACILITIES, INFORMATION TECHNOLOGY RESOURCES AND SENSITIVE INFORMATION

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and Task Order performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) Information in Attachment J, describes how contractors must handle sensitive but unclassified information. DHS MD 4300 Information Technology Systems Security in Attachment K and DHS 4300A Sensitive Systems Handbook prescribe policies and procedures

on security for IT resources. The TIP Contractor shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources, or sensitive information. The TIP Contractor shall not use or redistribute any DHS information processed, stored, or transmitted by the TIP Contractor, except as specified in the Task Order.

H.7.4.3 SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this task order are being implemented and enforced. The TIP Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Client Representative, and other Government oversight organizations, access to the TIP Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this task order. The TIP Contractor shall contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access will be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

H.7.4.4 HSAR 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

The contractor shall be responsible for IT security for all systems connected to a DHS network or operated by the contractor for DHS, regardless of location. This clause applies to all or any part of the Task Order that includes IT resources or services for which the contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The contractor shall provide, implement, and maintain an IT Security Plan. The Plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

- Within 30 Calendar days after award, the TIP Contractor shall submit for approval the IT Security Plan, which shall be consistent with and further detail the approach contained in the Contractor's proposal. The Plan, as approved by the Contracting Officer, shall be incorporated into the Task Order as a compliance document.
- The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), the Government Information Security Reform Act of 2000, the Federal Information Security Management Act of 2002, and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.
- The IT Security Plan shall specifically include instructions regarding handling and protecting sensitive information at the contractor's site (including any information stored,

processed, or transmitted using the contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include —

- Acquisition, transmission, or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted.
- Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

At the expiration of the Task Order, the TIP Contractor shall return all sensitive DHS information and IT resources provided to the TIP Contractor during the period of performance, and certify that all non-public DHS information has been purged from any TIP Contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

The TIP contractor shall submit written proof of IT Security accreditation to DHS for approval for all DHS approved technologies. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the Task Order as a compliance document. The TIP Contractor shall comply with the approved accreditation documentation.

H.7.4.5 HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee).
- Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized

official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee).

- Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest.
- Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

TIP Contractor employees working on this contract must complete all security forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

ALTERNATE II
(JUN 2006)

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs to all contracts and subcontracts:

Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

H.7.4.4 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

All unclassified IT resources shall be managed and controlled in compliance with HSAR clause 3004.470: Security Requirements for Access to Unclassified Facilities, Information Technology Resources and Sensitive Information.

H.7.4.5 CONTRACTOR EMPLOYEE ACCESS

All contractor employee access shall be managed and controlled in compliance with HSAR clause 3052.204-70; Security requirements for access to unclassified facilities, information technology resources and sensitive information.

H.7.4.6 ADDITIONAL INFORMATION FOR CLASSIFIED TASK ORDERS

All TIP Contractor handling of classified information shall be controlled in accordance with the DD Form 254 and comply with the following clauses in accordance with FAR 52.204-2 Security Requirements (Aug 1996).

H.7.5 PERSONNEL SECURITY CLEARANCE PROCESSING

The Security Clearance process begins with the submittal of an initial request to determine if the candidate has a DHS entry on duty clearance or required Security Clearance on file with DHS and or JPAS. To verify this, the Personnel Security Division (PSD) of DHS will verify what an individual has with DISCO (Defense Industrial Security Clearance Office) via the OPM portal (JPAS).

Access to DHS resources begins with an Entry on Duty determination. An EOD is an "entry on duty determination." Anyone (risk level or clearance) can receive an EOD (favorable or not). If the personnel security division (CSO/PSD) of DHS is unable to grant initial suitability/reciprocity (CSO/PSD) may need additional documentation to address any concerns that may arise; CSO/PSD may need to wait for an investigation, CSO/PSD will make an EOD determination. Listed are the steps one must follow for processing personnel security clearance requirements:

Reciprocity: If an individual is coming from a Component or other Federal Government Agency and they have an in scope investigation and were found suitable with that component or federal

agencies at the same risk level or with the same clearance level that they need and the in scope investigation meets or exceeds what is required for their new position your clearance can be processed as reciprocity. No matter where an individual is coming from their clearance/investigation information must be reflected in JPAS (DISCO). Not all agencies report to DISCO.

H.7.5.1 STEPS FOR PROCESSING SECURITY CLEARANCES

Step One: The TIP Contractor will submit to the St. Elizabeths DHS Special Program Office (SPO) the candidates full name (First, Middle, Last), Social Security Number (SSN), position, and current security clearance access level requirements (EOD, Secret, Top Secret, Top Secret with Sensitive Compartmented Information (SCI)). For those candidates that will only require an EOD, the TIP Contractor must type EOD and include a risk level of Moderate or High (High is for more stringent evaluation).

**********EXAMPLE**********
****

Position	Name	SSN	DOB	Current Clearance
Project Manager	John Smith	111-11-1111	01/01/1969	TS
Project Coordinator	Norma Rae Jean	222-22-2222	03/03/1972	Risk Moderate

**********EXAMPLE**********
****

Note: The request should only include either a Risk (for EOD only) or Clearance Level (for clearance request).

Step Two: The DHS St. Elizabeths SPO will coordinate with the Chief Security Office, Personnel Security Division for processing the clearance request.

Step Three: CSO/PSD will perform an initial check with JPAS to determine if the candidate has a clearance and to perform the initial suitability check. This process will ensure that if a candidate does not have a clearance then proper notification can be sent to the contractor security office.

Step Four: If the candidate has an active security clearance or EOD on file, DHS St. Elizabeths SPO will be provided DHS Form 11000.25 to initiate final DHS security clearance adjudication:

If there is "NOT" an active security clearance or EOD on file, the contractor will be required to sponsor/ initiate the security clearance process.

H.7.5.2 ELECTRONIC DHS FORM 11000.25

DHS Form 11000.25 is the document used for processing, adjudicating, and granting security clearances and access to DHS technologies, systems, and facilities. DHS Personnel Security Division (PSD) will only accept DHS 11000.25 forms submitted by DHS Contract Officer (CO), TPOC or designated representative)s, or Federal Points of Contact (POCs). DHS11000.25 forms submitted electronically by TIP Contractor Employees or the TIP Contractor company representatives will not be processed. Listed are the procedures required for submittal:

H.7.5.3 CONTRACT DD 254

A DD254 must be on file to process Secret/Top Secret/TS SCI clearance request. The DD254 must be provided to the Contracting Officer and on file otherwise the cases would be rejected.

H.7.5.4 ACTIVE SECURITY CLEARANCE OR EOD ADJUDICATION PROCESS

- 11000.25 is submitted by sponsoring CO via the TPOC or designated representative with accurate and complete information to the OCIO Security Officer
- E-Qip/Required Documents is emailed directly to prospective contract applicant
- Applicant completes the instructions to initiate the EOD process
- Applicant schedules an appointment to be fingerprinted
- Applicant will then submit his or her Security Packet onto the OCIO Security Officer.
- OCIO Security Officer performs a review of the documents and notify Personnel Security Division (PSD) * clock starts here
- Sponsoring TPOC or designated representative receives EOD Determination for applicant (Approved and or Delayed)from Personnel Security via email
- Approved TIP Contractor is required to attend Security Tuesday
- If badge/DHS equipment is required, a 3130 as in Attachment L will be submitted with complete and accurate information by the sponsoring TPOC or designated representative to the OCIO Security Officer
- Once the 3130 is completed, the approved TIP Contractor schedules badge appointment in Time Trade
- Contractor forwards confirmation email of appointment to OCIO Security Officer (required)
- 1100.14 form is distributed on the day of contractor’s appointment
- Once TIP Contractor terminates/separates, the Separation Form is completed by TPOC or designated representative and submitted to the OCIO Officer.

H.7.5.5 NON ELIGIBILITY AND EOD DELAY

For those needing TS/SCI who only have a TS, CSO/PSD will EOD delay until they receive the investigation and upon receipt we will adjudication for TS SCI eligibility.

If DHS receives a request for someone needing a clearance and they have what they need through JPAS, however, financial/criminal concerns come about in preliminary checks, DHS can EOD delay pending issue resolution.

H.7.5.6 DHS OFFICE OF SECURITY CUSTOMER SERVICE

For additional questions concerning the DHS forms, please contact the DHS Office of Security Customer Service at 202-447-5010 or email OfficeofSecurity@dhs.gov.

H.7.6 INFORMATION ASSURANCE (IA)

Access to DHS systems will be granted in accordance with MD 4300.1 for "dot-GOV". and USCG Commandant Instructions (COMDT INST) 5503.13 (Commandant Information Assurance for .mil) in Attachment M. All data and system software is the property of the DHS and may only be used in the performance of official Government business, more specifically, in support of the DHS and this Task Order.

H.7.7 DHS SPECIFIC SECURITY REQUIREMENTS

The Campus is a full Interagency Security Committee (ISC) Level 5 secured Campus. In the Performance Work Statement required under this Task Order, all TIP Contractor personnel must present proper identification to gain access to occupied building areas housing federal operations. TIP Contractor personnel include TIP Contractor employees and TIP Contractor subcontractor employees at all tiers. All TIP Contractors are required to meet standards and guidelines set forth in the U.S. Government HSPD-12 program.

TIP Contractor personnel requiring daily/weekly access to occupied building areas housing Federal operations over a period of 180 Calendar days or more shall undergo background investigations conducted by the United States Government, and will be issued Government-wide standard secure and reliable forms of identification (i.e., federal personal identity verification (PIV) credentials) as required under Homeland Security Presidential Directive-12 (HSPD-12). Credentialed TIP Contractor personnel must wear their PIV credential cards visibly above the waist at all times while in occupied building areas housing Federal operations.

All other TIP Contractor personnel requiring access to occupied building areas housing Federal operations will be issued visitor badges upon entry, must wear their visitor badges visibly above the waist, and must surrender their visitor badges upon exit.

All non-PIV credentialed TIP Contractor personnel must be escorted at all times (including after hours) while in occupied building areas housing federal operations. The escort must be a PIV credentialed individual who has been found suitable after completion of the required background investigation. An exception to this requirement will be provided for TIP Contractor personnel requiring daily/weekly access to occupied building areas housing federal operations, over a

period exceeding ten (10) Calendar days but less than 180 Calendar days. These individuals shall undergo a law enforcement check. Those who receive favorable results will be granted unescorted access to specified building areas. Those who receive unfavorable results will be denied any access to occupied building areas housing Federal operations, pending completion of any adjudication and/or appeal process or final determination.

The minimum clearance required is HSPD-12 Entry of Duty security evaluation. Designated Key Personnel shall be cleared at the TS/SCI or are eligible for TS/SCI clearance. Non-U.S. citizens have to be approved individually by DHS.

H.7.8 DHS SPECIFIC INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

The TIP Contractor is responsible for DHS approved Information Technology (IT) security for all personnel with access to the DHS network, systems connected to the DHS network, or those systems developed and/or operated by the contractor for DHS. This clause is applicable to all or any part of the task order that includes information technology resources or services in which the contractor may have physical or electronic access to DHS information contained in its systems. This includes but is not limited to information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include but are not limited to acquisition, transmission, or analysis of data owned by DHS or access to DHS networks or computers at a level beyond that granted the general public (e.g., bypassing the DHS firewall).

The TIP Contractor, its subcontractors, and the employees of each must sign a confidentiality agreement at any time prior to or during the performance of this task order at the direction and discretion of the Contracting Officer.

All TIP Contractor employees with network access must review the Security Awareness Website on an annual basis and provide electronic verification of their review within five (5) business days after the anniversary of the effective date of the Task Order. The TIP Contractor shall verify/represent annually that all contractor employees having network access have complied with the security requirements. This certification shall be provided to the COR/TPOC or designated representative by email or in writing within five (5) business days after the anniversary of the effective date of the contract. Failure to complete the review and certification may result in revocation of network access privileges and possible removal of the individual employees from the task order.

H.7.9 DHS ACCESS REQUIREMENTS

The TIP Contractor shall allow DHS, including the Office of Inspector General, access to the TIP Contractor's and all subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the Task Order. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data,

systems, software, and hardware or to the function of computer systems operated on behalf of DHS or the network accessed by the contractor personnel and to preserve evidence of computer crime or misuse.

H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON- DISCLOSURE REQUIREMENTS

H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the TIP Contractor is currently providing support or anticipates providing support to GSA PBS or DHS that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The TIP Contractor is also required to complete and sign an Organizational Conflict of Interest (OCI) Statement in which the contractor (and any Subcontractors, consultants or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any TOR relating to any work in the Task Order. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.9.2 NON DISCLOSURE REQUIREMENTS

If this Task Order requires the TIP Contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include Subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the Task Order:

- Execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form prior to the commencement of any work on the Task Order and

- Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor proposal information, or source selection information.

All proposed replacement contractor personnel also must submit a Non-Disclosure Agreement and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this Task Order or obtained by the Government is only to be used in the performance of the Task Order. The TIP Contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.18 CONTRACTOR'S PURCHASING SYSTEMS

The objective of a TIP Contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a Task Order the Contracting Officer shall verify the validity of the contractor's purchasing system. Thereafter, the TIP Contractor is required to certify to the

Contracting Officer no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the Contracting Officer within two (2) weeks from the date the results are known to the TIP Contractor.

H.24 TOOLS & ODCS

The Government will require the TIP Contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the Task Order. Such requirements will be identified at the time a Task Order is issued or may be identified during the course of a Task Order, by the Government or the contractor. If the TIP Contractor initiates a purchase within the scope of this Task Order, the TIP Contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP). The RIP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR.

H.25 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the TIP Contractor acquires hardware/software maintenance support, all licenses, maintenance agreements, and/or contractual rights to receive title shall be turned over to the Government upon completion of the Task Order.

The Government's liability to reimburse the TIP Contractor for costs incurred from the acquisition of hardware/software maintenance support SHALL BE LIMITED to costs incurred during the period of the order for which the Government received the hardware/software maintenance support acquired by the contractor on a cost reimbursable, fee basis.

H.26 AWARD FEE

Refer to Award Fee Determination Plan in Attachment N.

H.26.1 ESTABLISHMENT AND DETERMINATION OF AWARD FEE

The award fee dollar pool will be established on execution of the Task Order. The Government reserves the right to adjust these amounts to reflect any change in the Estimated Cost. The amount of Award Fee that can be earned cannot exceed (b) (4) (b) (3)) *(Note: award fee percentage added at award)* of the estimated labor cost established for each CPAF CLIN.

The Government will, at the conclusion of each specified evaluation period(s), evaluate the contractor's performance for a determination of award fee earned. The TIP Contractor agrees that the determination as to the amount of the award fee earned will be made by the Government Award Fee Determining Official (AFDO) and such determination is binding on both parties and shall not be subject to the "Disputes" clause or to any board or court.

The evaluation of contractor performance will be in accordance with the Award Fee Determination Plan (AFDP). The Government will promptly advise the contractor in writing of the determination and reasons why the award fee was not earned. The TIP Contractor may submit a self-evaluation of performance for each period under consideration. While it is recognized that the basis for the determination of the fee will be the evaluation by the Government, any self-evaluation which is received within ten (10) business days after the end of the period being evaluated may be given consideration as deemed appropriate by the AFEB. Any cost associated with the development and presentation of a self-evaluation will not be allowed as a direct cost to this Task Order.

H.26.2 AWARD FEE DETERMINIATION PLAN (AFDP)

An Award Fee Determination Plan (AFDP) will be established by the Government, in consultation with the contractor, based on the objectives and concerns provided in the Task Order and the contractor-provided solutions. The AFDP will include the criteria used to evaluate each area and the percentage of award fee available for each area. The initial plan will be finalized NLT three (3) weeks after award date.

The AFDP may be revised unilaterally by the Government at any time during the period of performance. The Government will make every attempt to provide changes to the contractor 15 business days prior to the start of the evaluation period to which the change will apply. The AFDP may be reevaluated each evaluation period, with input from the contractor.

The Government may, at its option, unilaterally revise the plan to include metrics gathered from the re-evaluation to be applied in future award fee periods.

H.26.4 DISTRIBUTION OF AWARD FEE

Award Fee will be distributed in accordance with the AFDO determination and the AFDP.

If the Government initiates any action that impacts the contractual scope of work and/or schedule pursuant to the “changes” clause or other pertinent provisions of the Task Order, the maximum award fee available for payment for any evaluation periods impacted will be modified as negotiated between the parties.

H.27 GOALS FOR SUBCONTRACTING

The Government is committed to ensuring that small, HUBzone, small disadvantaged, women-owned, veteran-owned, and service-disabled veteran owned small business concerns are provided maximum practicable opportunity to participate as subcontractors in the performance of the Task Order.

Accordingly, the goals for TIP Contractor-planned subcontracting dollars on orders amortized over the reporting periods of each Individual Subcontractors Report (ISR) are stated as follows:

SMALL BUSINESS	**(b) ___ percent**	

HUBzone Small Business		(b) (4) _ percent
Small Disadvantaged Business		(b) (3) _ percent
Women-Owned Small Business		_ percent
Veteran-Owned Small Business		_ percent
Service-Disabled Veteran-Owned Small Business		_ percent

The minimal individual goals of HUBzone Small Business, Small Disadvantaged Business, Women-Owned Small Business, Veteran-Owned Small Business, and Service-Disabled Veteran-Owned Small Business are a subset of the (b) small business goal. Subcontracting credit will only be given to first tier subcontracts.

FAR 19.704(a)(9) requires that the TIP Contractor include FAR 52.219-8, "Utilization of Small Business Concerns" in all subcontracts that provide further subcontracting opportunities. The TIP Contractor must require all subcontractors, except small business concerns, that receive subcontracts in excess of $650,000 ($1,000,000 for construction) to adopt a plan that complies with the requirements of the clause at FAR 52.219-9, "Small Business Subcontracting Plan.")

Reporting and Cooperation -

* FAR 19.704 (a) (10) requires assurances that the TIP Contractor shall:
(1) Cooperate in any studies or surveys as may be required,
(2) Submit periodic reports so that the Government can determine the extent of compliance by the Contractor with the subcontracting plan;
(3) submit the Individual Subcontracting Report (ISR), and the Summary Subcontract Report (SSR);
(4) Ensure that its subcontractors with subcontracting plans agree to submit the ISR and/or the SSR;
(5) Provide its prime contract number and its DUNS number and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports, to all first-tier subcontractors with subcontracting plans; and
(6) Require that each subcontractor with a subcontracting plan provide the prime contract number and its own DUNS number, and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports, to its subcontractors with subcontracting plans.

These reports must be received within 30 days after the close of each calendar period. That is:

Calendar Period	Report Due	Date Due	Send Report To
10/01--03/31	ISR	04/30	Contracting Officer with copy to bscncr@gsa.gov
04/01--09/30	ISR	10/30	Contracting Officer with copy to bscncr@gsa.gov
10/01--09/30	SSR	10/30	Contracting Officer with copy to Janice.keys@gsa.gov

Recordkeeping -

FAR 52.219-9(d)(11) requires a list of the types of records your company will maintain to demonstrate the procedures adopted to comply with the requirements and goals in the subcontracting plan. These records include, but are not limited to, the following:

The contractor shall maintain the following types of records on a [company-wide] [division-wide] basis:

Source lists, guides, and other data that identify SB, VOSB, SDVOSB, HSB, SDB, and WOSB;

Records that identify organizations contacted in an attempt to locate SB, VOSB, SDVOSB, HSB, SDB, and WOSB sources;

Records on each subcontract solicitation resulting in an award of more than $100,000 indicating: (1) whether SB were solicited, and if not, why not; (2) whether VOSB were solicited, and if not, why not; (3) whether SDVOSB were solicited, and if not, why not; (4) whether HSB were solicited, and if not, why not; (5) whether SDB were solicited, and if not, why not; (6) whether WOSB were solicited, and if not, why not; and (7) if applicable, the reason that the award was not made to a small business concern;

Records of outreach efforts, e.g., contacts with trade associations, business development organizations, veterans service organizations; attendance at conferences and trade fairs to locate SB, HSB, SDB, and WOSB sources;

Records of internal guidance and encouragement provided to buyers through: (1) workshops, seminars, training, etc.; and (2) monitoring performance to evaluate compliance with the program's requirements; include the following paragraph unless you have a commercial plan.

On a contract-by-contract basis, records to support subcontract award data including the address, and business size of each subcontractor;

Additional Records: NARRATIVE

_____

_____

In addition to the requirements set forth in H.10 of the basic contract for submission of ISRs and SSRs on the basic contract, the ISRs and SSRs are required specifically covering this Task Order in order to allow GSA and DHS to capture the information on small, small disadvantaged and women-owned small business participation in this program.

H.28 SERVICE LEVEL AGREEMENTS (SLAS) AND PERFORMANCE METRICS

The use of well-defined, measurable Service Level Agreements (SLAs) is a key success factor for providing and managing services under this Task Order. The TIP Contractor shall propose SLAs in their proposal response. During Phase 1, the TIP Contractor and the Government will

work together to jointly refine and/or define new SLAs for specific functional areas. Listed below is the Service Level Agreement and Metrics program DHS desires to use as a foundation from which to develop, refine, and expand SLAs and corresponding metrics. It is expected that the TIP Contractor shall improve and expand upon the listed SLA program.

The Government realizes that the Campus environment is dynamic, and SLAs may need to be revised periodically throughout the Task Order period of performance. The Government retains the right to unilaterally modify SLAs.

The TIP Contractor shall establish a performance management and accountability program. This program shall be comprised of objective operational performance metrics, and include the methodology for how these metrics can be captured and reported.

H.28.1 PERFORMANCE REPORTING

Reporting shall be based on technology monitoring, observation, and self-assessment. Reports will be subjected to a formal review, analysis, and approval. The reporting schedule shall be based on weekly, monthly, and quarterly reports. Weekly reporting shall be performed by the vendor, monthly reports shall be presented to the St. Elizabeths Governance Board, and quarterly reporting shall be presented to DHS/GSA senior management.

H.29 CONTRACT ADMINISTRATION

Contracting Officer (CO):

Gregory Lee, CO
GSA FAS AAS FEDSIM
1800 F Street, NW, 3100
Washington, DC 20405
Telephone: (202) 357-5831
Email: greg.lee@gsa.gov

Contracting Officer Representative (COR):

Dustin Dunn
GSA FAS AAS FEDSIM
1800 F Street, N.W.
Washington, D.C. 20405
Telephone: (202) 304-4745
Email: dustin.dunn@gsa.gov

Technical Point of Contact (TPOC) – DHS:

Kevin Sullivan
DHS/CRSO/OS
2701 Martin Luther King Ave SE,
Washington, DC 20032
Phone: 202-561-4904
Email: kevin.sullivan@hq.dhs.gov

Technical Point of Contact (TPOC) – USCG:

LCDR Dana Schulman
U.S. Coast Guard Base National Capital Region
Attn: C4IT Department Stop 7118
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7118
Telephone: 202.372.4006
E mail: dana.e.schulman@uscg.mil

H.30 DATA RIGHTS

The Government intends to only use Commercial off-the-shelf (COTS) and Government off-the -shelf (GOTS) software. However, FAR clause at 52.227-17, Rights in Data -- Special Works (Dec 2007), shall apply to any and all data (as defined in FAR 52.227-17) first produced in the performance of this Task Order, including without limitation any derivative works (as such term is defined in 17 U.S.C. §101) based upon the COTS or GOTS software provided under this Task Order and any associated source code and documentation. Upon creating any such data, the Contractor shall deliver it to the Government, shall assign the copyright in such data to the Government and shall retain no rights therein.

If the TIP Contractor proposes to provide commercial computer software ("Commercial Software") as part of its proposed solution in response to this Task Order, the TIP Contractor shall ensure that any software license agreement ("License Agreement") associated with such Commercial Software and intended to bind the Government complies with the FAR clause at 12.212(a), which provides, in relevant part, that commercial computer software and documentation shall be acquired under licenses customarily provided to the public "to the extent such licenses are consistent with Federal law." The most common examples of areas of non-compliance are set forth in the table below, which is provided for information purposes only and does not constitute an exhaustive list.

The requirement to propose compliant License Agreements shall apply regardless of whether the original rights holder to the Commercial Software ("Licensor") is the offeror, its subcontractor, or a third party, in the case of third-party software embedded or provided with the Commercial Software. Further, this requirement shall apply regardless of the format or title of the License Agreement, i.e., whether entitled "Software License Agreement," "End User License Agreement," "Terms of Service," or otherwise and whether presented in hard copy or in a click wrap or other electronic format. For the avoidance of doubt, this may require the offeror to negotiate with its Licensors and to obtain a revised version of the License Agreement. License Agreements incorporated into a company's existing Schedule 70 or other Government contract are not exempt from this requirement.

If proposing Commercial Software, the offeror shall include a statement in its proposal certifying that all applicable License Agreements will comply with the requirement. Actual License Agreements need not be submitted prior to award. Failure to certify

compliance will render the proposal ineligible for award, and non-compliance identified after award may entitle the Government to terminate the contract and seek any or all available remedies for breach of contract.

Commercial Terms*	Legal Restriction	Action**
Contract formation and modification	Under FAR 1.601(a), in an acquisition involving the use of appropriated funds, an agreement binding on the Government may only be entered into by a duly warranted contracting officer in writing. Under FAR 43.102, the same requirement applies to contract modifications affecting the rights of the parties.	Any provisions purporting to form a contract binding on the US Government by any other means (e.g., use, download, click through terms, etc.) must be deleted. The same applies to provisions allowing for License Agreement terms to be changed unilaterally by the Licensor.
Patent or other type of intellectual property Indemnity – sellers of products or services often provide that in the event of claim or litigation alleging infringement of patent rights asserted by some third party that the seller will indemnify the buyer, provided that the buyer provide notice of the claim or litigation, and that the seller assume control of the litigation and any proposed settlement.	Under the authority of 28 USC § 516, only the Attorney General, acting by and through the attorneys of the US Department of Justice, may represent the US Government in litigation.	The patent or other type of intellectual property indemnity clause remains in effect, but any undertaking to "defend" the Government or any requirement that the seller control litigation and/or any proposed settlement is to be deleted.

General Indemnity – sellers of products or services provide that in the event of any litigation arising from the buyers use of the product or service that buyer will indemnify seller's litigation costs and damages (if any).	Agreements to pay the attorney fees of a private party require a statutory waiver of sovereign immunity. Agreements to pay some indeterminate amount of money in the future violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 USC §11.	General Indemnity clauses must be removed from the License Agreement.
Arbitration of disputes – sellers of products or services provide that any disputes with buyer must be resolved through binding arbitration without recourse to litigation in state or federal courts.	Federal Agencies are not allowed to use binding arbitration unless the head of the agency has promulgated guidance through administrative rulemaking on the use of binding arbitration. *See* 5 USC § 575. At the time of this TOR release, GSA has not done so.	Binding Arbitration clauses must be removed from the License Agreement.
Venue, Jurisdiction and Choice of Law – sellers of products or services provide that jurisdiction of any dispute will be in a particular state, federal or foreign court or that particular state or foreign law will govern.	Litigation where the US Government is a defendant must be heard either in US District Court (28 USC § 1346) or the US Court of Federal Claims (28 USC §1491). The US Government, as the sovereign, does not contract under state or foreign law. Depending on the subject matter of the	Clauses claiming that disputes will only be heard in state court will be revised to allow disputes in Federal court. Choice of law clauses must be deleted.

	dispute, the Contract Disputes Act or other applicable law will govern.	
Equitable Remedies – sellers of products or services provide that in the event of a dispute concerning patent or copyright infringement that the end-user agree that an injunction is appropriate.	The only remedy provided for copyright or patent infringement against the US Government is monetary damages. *See* 28 USC § 1498.	Equitable remedy clauses must be removed.
Negative Options – sellers of products or services provide that option periods will automatically be exercised unless affirmative action is taken by the buyer to not exercise the option.	Agreements to pay money in advance of appropriations violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 USC §11.	Negative option clauses must be removed.
Limitation of Liability	Various (see next column)	Limitation of liability clauses may be included in accordance with the Licensor's standard commercial practices, except that such clauses may not operate to impair or prejudice the U.S. Government's right (a) to recover for fraud or crimes arising out of or relating to this Task Order under any Federal fraud statute, including

		without limitation the False Claims Act (31 USC §§3729 through 3733), or (b) to express remedies provided under any FAR, GSAR or master Alliant contract clauses incorporated into this Task Order.
Integration/Order of Precedence Clauses		Any provisions purporting to invalidate or supersede the terms of the Government Task Order resulting from this TOR (such provisions are frequently found in "entire agreement" clauses) must be removed from the License Agreement.

* The following standard commercial terms are deemed non-compliant within the meaning of this clause

** The License Agreement will be deemed compliant when the action specified in this column is successfully implemented

H.31 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, "the data rights provisions in FAR 52.227-14 apply.

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section I of the contractor's Alliant) Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

I.2 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) SOLICITATION CLAUSES (http://www.arnet.gov/far/)

This Task Order incorporates one more clauses by reference with the same force and effect as if they were given in full text. Upon request the Contracting Officer will make their full text available. Also, the full text of a provision may be accessed electronically at these addresses:

FAR website: https://www.acquisition.gov/far/
GSAM website: https://www.acquisition.gov/gsam/gsam.html

CLAUSE NO	CLAUSE TITLE	DATE
52.204-2	SECURITY REQUIREMENTS	(AUG 1996)
52.204-11	AMERICAN RECOVERY AND REINVESTMENT ACT-REPORTING REQUIREMENTS	(JULY2010)
52.215-21	REQUIREMENTS FOR CERTIFIED COST OR PRICING DATA OTHER THAN COST OR PRICING DATA – MODIFICATIONS	(OCT 2010)
52.216-8	FIXED FEE	(MAR 1997)
52.217-8	OPTION TO EXTEND SERVICES Fill-In Date: 60 Days of the Start Date of the Option	(NOV 1999)
52.217-9	OPTION TO EXTEND THE TERM OF THE CONTRACT Fill-In Date: 60 Days of the Start Date of the Option Fill-In Date: 30 Days Fill-In Date: 7 Years	(SEP 2006)
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	(JAN 2011)
52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN	(JAN 2011)
52.223-15	ENERGY EFFICIENCY IN ENERGY CONSUMING PRODUCTS	(DEC 2007)
52.223-16	IEEE 1680 STANDARD FOR THE ENVIRONMENTAL ASSESSMENT OF PERSONAL COMPUTER PRODUCTS	(DEC 2007)
52.227-14	RIGHTS IN DATA – GENERAL ALTERNATE IV	(DEC 2007)
52.227-15	REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE	(DEC 2007)
52.227-16	ADDITIONAL DATA REQUIREMENTS	(JUN 1987)
52.227-17	RIGHTS IN DATA SPECIAL WORKS	(DEC 2007)

52.227-21	TECHNICAL DATA DECLARATION REVISION AND WITHHOLDING OF PAYMENT – MAJOR SYSTEMS	(DEC 2007)
52.232-18	AVAILABILITY OF FUNDS	(APR 1984)
52.232-20	LIMITATION OF COSTS	(APR 1984)
52.232-22	LIMITATION OF FUNDS	(APR 1984)
52.244-2	SUBCONTRACTS	(OCT 2010)
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	(DEC 2010)
52.251-1	GOVERNMENT SUPPLY SOURCES	(AUG 2010)

52.244-2 Subcontracts.

As prescribed in 44.204(a)(1), insert the following clause:

SUBCONTRACTS (OCT 2010)

(a) ***Definitions***. As used in this clause—

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that—

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds—

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

_____

_____

_____

(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting—

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason certified cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (b), (c), or (d) of this clause.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination—

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

Subcontractor Name	Description of Support to be Provided
(b) (4) (b) (3)	

Subcontractor Name	Description of Support to be Provided
(b) (4) (b) (3)	[redacted]

Subcontractor Name	Description of Support to be Provided
(b) (4) (b) (3)	[redacted]

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

CLAUSE NO	CLAUSE TITLE	DATE
552.232.25	Prompt Payment Clause	(Nov 2009)

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section J of the TIP Contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

J.1 LIST OF ATTACHMENTS

Attachment A	Acronym Listing
Attachment B	Infrastructure Change Control Board
Attachment C	Interagency Security Committee - Security Standards for Federal Buildings (FOUO)
Attachment D	DHS Technical Refresh Model (FOUO)
Attachment E	DHS Operations Centers (SBU)
Attachment F	Program Governance (FOUO)
Attachment G	DD254
Attachment H	4300A v7.2.1 DHS Sensitive Systems Handbook
Attachment I	4300B DHS NSS Handbook v6
Attachment J	11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information (FOUO)
Attachment K	4300.1 Information Technology Systems Security
Attachment L	Form 3130
Attachment M	USCG Commandant Instructions 5503.13 (FOUO)
Attachment N	Award Fee Determination Plan dated 12/6/2017
Attachment O	Project Staffing Plan Template
Attachment P	Example SLA Format
Attachment Q	Contractor Employee NDA
Attachment R	Travel Authorization Request
Attachment S	St. Elizabeths Control Systems Network Diagram
Attachment T	GSA PBS SBU Policy Letter
Attachment U	St. Elizabeths Security System Market Survey Report
Attachment V	IT Master Plan – PON Conceptual Layout
Attachment W	WBS and Dictionary
Attachment X	St. Elizabeths Infrastructure Equipment List
Attachment Y	Executive Level Schedule
Attachment Z	2009 DHS IT Strategic Plan
Attachment AA	Enclave Security Technical Integration Guide v4
Attachment BB	St. Elizabeths East Campus North Parcel
Attachment CC	Voice and Video over Internet Protocol (VVoIP) Security Technical Integration v3
Attachment DD	Security Master Plan
Attachment EE	Facilities Standards for PBS
Attachment FF	Deliverable Review Process
Attachment GG	DHS Site Security Guide
Attachment HH	SCIF Cabling Standards (SBU)
Attachment II	Programmatic Agreement
Attachment JJ	St. Elizabeths Volumetrics
Attachment KK	DHS Cable Standard (FOUO)

Attachment LL	USCG Construction Document
Attachment MM	Media Sanitization NISTSP900-88 Revision 1
Attachment NN	EMP and TEMPEST Risks
Attachment OO	DoD Video Teleconferencing Standards
Attachment PP	DHS AV/VTC Standards (FOUO)
Attachment QQ	DHS DOC IT Security Distribution DID (SBU)
Attachment RR	SCIF Conduit and Classification Standards (SBU)
Attachment SS	Key Personnel Staffing Matrix
Attachment TT	Task Order Funding Table

Attachment T

This page intentionally left blank.

CLIN	CLIN TYPE	COST OVERRUN	ESTIMATED	ESTIMATED BASE FEE or	ESTIMATED	TOTAL		FUNDED BASE FEE or	FUNDED	
		(b) (4)	(b) (3)							
0001A	Task 1 – Base Year– 6/6/11 throu 01/27/12									
0001B	Task 1 – Base Year – 01/28/12 through 06/05/12									
1001	Task 1 – Optional Period 1									
2001	Task 1 – Optional Period 2									
3001A	Task 1 – Optional Period 3 – 6 Jun 2014 to 5 December 2014									
3001B	Task 1 – Optional Period 3 – 6 December 2014 to 5 June 2015									
4001A	Task 1 – Optional Period 4 – 6 Jun 2015 to 5 December 2015									
4001B	Task 1 – Optional Period 4 – 6 December 2015 to 5 June 2016									
5001	Task 1 – Optional Period 5 – 6 Jun 2016 to 5 June 2017									
5001A	Task 1 – Optional Period 5 – 6 Jun 2016 to 5 Decmber 2016									
5001B	Task 1 – Optional Period 5 – 6 December 2016 to 5 June 2017									
6001	Task 1 – Optional Period 6 – 6 Jun 2017 to 5 June 2018									
6001A	Task 1 – Optional Period 6 – 6 Jun 2017 to 5 Decmber 2017									
6001B	Task 1 – Optional Period 6 – 6 December 2017 to 5 June 2018									
SUB										
1002	Task 2, Phase 1									
1002A	Task 2, Phase 1, ARRA									
1002B	Task 2, Phase 1, Non-ARRA									
SUB										
1003	Task 3, Phase 1									
1003A	Task 3 Phase 1, ARRA									
1003B	Task 3, Phase 1, Non-ARRA									
1004A	Task 4, Year 1									
1004B	Task 4, Year 2									
SUB										
2002	Task 2 Post Phase 1									
2002A	Task 2 - 6/2015-6/2016									
2002B	Task 2– Optional Period 5 – 6 Jun 2016 to 5 June 2017									
2002C	Task 2 - 6/2017-6/2018									
SUB										
2003	Task 3 Post Phase 1									

		(b) (4) (b) (3)
2003A	Task 3 - 6/2015-6/2016	
2003B	Task 3 – Optional Period 5 – 6 June 2016 to 5 June 2017	
2003C	Task 3 - 6/2017-6/2018	
SUB		
2004	Task 4 Post Phase 1	
2004A	Task 4 - 6/2015-6/2016	
2004B	Task 4 – Optional Period 5 – 6 June 2016 to 5 June 2017	
2004C	Task 4 - 6/2017-6/2018	
SUB		
0005	Task 5 – Base Year	
1005	Task 5 – Option Year 1	
2005	Task 5 – Option Year 2	
3005	Task 5 – Option Year 3	
4005	Task 5 – Option Year 4: 6 June 2015 to 5 June 2016	
5005	Task 5 – Option Year 5: 6 June 2016 to 5 June 2017	
6005	Task 5 – Option Year 6: 6 June 2017 to 5 June 2018	
SUB		
0006	Task 6 – Base Year	
0006	Task 6 – Option Year 1	
2006	Task 6 – Option Year 2	
3006	Task 6 – Option Year 3	
4006	Task 6 – Option Year 4: 6 June 2015 to 5 June 2016	
5006	Task 6 – Option Year 5: 6 June 2016 to 5 June 2017	
6006	Task 6 – Option Year 6: 6 June 2017 to 5 June 2018	
SUB		
0007	Task 7 – Base Year	
1007	Task 7 – Option Year 1	
2007	Task 7 – Option Year 2	
3007	Task 7 – Option Year 3	
4007	Task 7 – Option Year 4: 6 June 2015 to 5 June 2016	
5007	Task 7 – Option Year 5: 6 June 2016 to 5 June 2017	
6007	Task 7 – Option Year 6: 6 June 2017 to 5 June 2018	
SUB		
0008	TOOLs Including Indirect Handling Rate 8.08%	
0008A	Tools ARRA SubCLIN	
0008B	Tools Non ARRA SubCLIN	
0008C	Tools Non ARRA SubCLIN: Option Year 4, 6 June 2015 to 5 June 2016	

(b) (4) (b) (3)

0008D	Tools Non ARRA SubCLIN: Option Year 5, 6 June 2016 to 5 June 2017	
0008E	Tools Non ARRA SubCLIN: Option Year 6, 6 June 2017 to 5 June 2018	
SU B		$
0009	ODCs Including Indirect Handling Rate 12.03%	
0009A	ODCs ARRA SubCLIN	
0009B	ODCs Non ARRA SubCLIN	
0009C	ODCs Option Year 4, 6 June 2015 to 5 June 2016	
0009D	ODCs Option Year 5, 6 June 2016 to 5 June 2017	
0009E	ODCs Non ARRA SubCLIN: Option Year 6, 6 June 2017 to 5 June 2018	
SUB		$
0010	Long Distance Travel	
1010	Long Distance Travel: Option Year 4, 6 June 2015 to 5 June 2016	
2010	Long Distance Travel: Option Year 5, 6 June 2016 to 5 June 2017	
3010	Long Distance Travel: Option Year 6, 6 June 2017 to 5 June 2018	
SUB		
0011-3011	Contract Access Fee - Base Period and Option Periods 1-3	
4011	Contract Access Fee - Option Period 4: 6 June 2015 to 5 June 2016	
5011	Contract Access Fee - Option Period 5: 6 June 2016 to 5 June 2017	
6011	Contract Access Fee - Option Period 6: 6 June 2017 to 5 June 2018	
SUB		
	Non-Severable CLINs	
9002A	JCSC Task 2: Non-Severable (Requirements Analysis & Design)	
9002B	Task 2 - Requirement Analysis & Design	
9002C	Physical Security Non-Severable (Requirements Analysis & Design)	
9003A	JCSC Task 3: Non-Severable (Implement & Test Solution)	
9003B	Task 3 Implement & Test Solution	
9003C	Physical Security: Non-Severable (Implement & Test Solution)	
9008A	JCSC Task 8: Non-Severable (Tools) / Indirect Handling Rate 8.08%)	

(b) (4) (b) (3)

9008B	TOOLs/ Including Indirect Handling Rate 8.08%	[redacted]	[redacted]
9008C	Physical Security Task 8: Non-Severable (Tools) / Indirect Handling Rate 8.08%)	[redacted]	[redacted]
SUB		[redacted]	[redacted]
TOTAL		(b) (4) (b) (3) [redacted]	$284,314,643